Grayson College Password Policy

Information Technology: Policy IT-02
Effective Date: 11/10/17
Last Revision Date: 11/10/17

Contents

I. Purpose/Scope

The purpose of this policy is to establish the applicability of, and specific responsibilities relating to, the *GC Password Strength and Security Standards* (Password Standards [1]). This policy applies to all passwords that provide access to GC electronic information resources.

II. Definitions

The following terms used in this policy are defined in the online *Glossary of GC IT Policy-Related Terms*, available at http://www.grayson.edu/employee-resources/policies%20handbooks%20and%20guides.html

- Confidential Information
- Electronic Information Resources
- Restricted Data
- Subject Matter Expert
- System Steward

III. Detailed Policy Statement: Applicability and Responsibility

APPLICABILITY

1. Compliance with the GC Password Standards is required for passwords that provide access to College restricted data [2], or where otherwise required by law, GC or campus policy, or contract.

2. The Password Standards are also recommended for passwords that provide access to other types of confidential information.

3. Passwords that do not provide access to confidential information, and do not share an Authentication System with ones that do, are not required to comply with the Password Standards.

RESPONSIBILITY

System Stewards [2], in consultation with Subject Matter Experts [2], where appropriate, are responsible for determining the applicability of the Password Standards to systems or data for which they are responsible based on the above criteria [3]. In situations where it is not clear whether the Password Standards apply to a certain type of data or system, the System Steward shall err on the side of more secure password requirements. System Stewards are also responsible for ensuring implementation and enforcement of the Password Standards where they are applicable. This includes informing users of password requirements.

System Stewards of authentication systems (e.g. systems, such as an identity management system, that allow the same username/password to be used for access to multiple services) are responsible for including in their service definition the minimum level of protection required for passwords provided by their system(s), and for communicating this information to other System Stewards.

All individuals are responsible for following the Password Standards where required. This includes not using passwords that provide access to confidential information with other systems or applications that do not adhere to the Password Standards.

IV. Authority

The campus Vice President, Information Technology (IT VP) is the campus authority for the *GC Password Policy*. This policy was initially reviewed and approved by the IT VP on 11/1/17. Last update was 10/31/17. Next review date is January 2022.

V. Getting Help

For questions or feedback about this policy, contact the IT Department by visiting http://help.grayson.edu

VI. Related Standards

- GC Password Strength and Security Standards: http://www.grayson.edu/employee-resources/policies%20handbooks%20and%20guides.html

Footnotes:

[1] The GC Password Strength and Security Standards are available at http://www.grayson.edu/employee-resources/policies%20handbooks%20and%20guides.html

[2] See Definitions

[3] If a System Steward relies on an Authentication System, e.g. an identity management system, it is the responsibility of the System Steward to include password protection requirements of the Authentication System in this assessment.