Grayson College
Information Technology Services (GC-IT)

User Accounts Password Policy:

PURPOSE:
All user accounts will be protected by passwords that are both strong and confidential. Users will protect the security of those passwords by managing passwords according to GC-IT password procedures.

System and Application Administrators will ensure account passwords are secured using industry best practices.

SCOPE:
The GC User Accounts Password policy applies equally to all individuals granted access privileges to any Grayson College information technology resources.

POLICY:
Users are responsible for what is accessed, downloaded, or created under their credentials regardless of intent. An unauthorized person can cause loss of information confidentiality, integrity and availability that may result in liability, loss of trust, or embarrassment to GC.

Account holder's responsibilities:

1. Must create a strong password and protect it.
2. Password must have a minimum length of ten (10) alphanumeric characters.
3. Password must contain a mix of upper case, lower case and numeric characters and special characters (!@#%^&*+=?/~';:,<>|\).
4. Passwords must not be easy to guess, for instance, they should not include part of your social security number, your birth date, your nickname, etc.
5. Passwords must not be easily accessible to others (e.g. posted on monitors, under keyboards).
6. Computing devices must not be left unattended without locking or logging off of the device.
7. Stored passwords must be encrypted.
8. GC username and password should not be used for external services (e.g. LinkedIn, Facebook or Twitter).
9. Users should never share their password with anyone, including family, supervisors, co-workers and GC-IT personnel.

10. Users will be required to change passwords at least once per 120 days.
11. If you know or suspect that your account has been compromised, change your password immediately and contact GC-IT Service Desk for further guidance and assistance.
12. If GC-IT suspects your account has been compromised, your account will be deactivated and you will be contacted immediately.

Any individuals responsible for managing passwords must:

1. Prevent or take steps to reduce the exposure of any clear text, unencrypted account passwords that GC applications, systems, or other services have received for purposes of authentication.
2. Never request that passwords be transmitted unencrypted. It is particularly important that passwords never be sent via email.
3. Never circumvent this password policy for the sake of ease of use.
4. Coordinate with GC-IT regarding password procedures.

Detailed information and instructions for password management can be found on the GC website in the New Employee Technology Orientation training booklet. https://grayson.edu/employment/policies-handbooks-guides.html

DEFINITIONS:
Compromised Account: The unauthorized use of a computer account by someone other than the account owner.

Encrypted: The conversion of data into a form, called cipher text that cannot be easily understood by unauthorized people. Encryption is achieved using Windows native Bit Locker or other available software.

Password: A string of characters input by a system user to substantiate their identity, authority, and access rights to the computer system that they wish to use.

System Administrator: Individual(s) who are responsible for running/operating systems on a day-to-day basis.

Unauthorized person: A person who has not been given official permission or approval to access GC systems.

Related Policies, References and Attachments:

An index of approved GC-IT policies can be found on the GC Information Technology Services Policies website at https://grayson.edu/employment/policies-handbooks-guides.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the Policy Compliance Document. The GC Information Security Program and GC Information Security User Guide are also available on the Information Technology Services Policies website.