IT PASSWORD POLICY

IT PASSWORD POLICY			
Effective Date	May 19, 2016	**Policy Type**	Administrative
Responsibility	Director, Information Technology	**Cross- Reference**	1. Information Management, Data Classification, Handling and Retention Policy
Approver	Executive Council		
Review Schedule	Every 5 years	**Appendices**	1. Password Requirements

1. Policy Statement

1.1 An important aspect of computer security is the safeguarding of personal and confidential information of all individuals and organizations affiliated with Grande Prairie Regional College ("GPRC", or "the Institution"). Properly chosen passwords by Institution system users will assist in the control of access to systems and data.

2. Background

2.1 Poor password management can increase the risk of unauthorized access to the Institution's information systems and data. Ensuring that standards for password management are in place can reduce these risks.

3. Policy Objective

3.1 The objective of this policy is to define the acceptable standards for password management at the Institution.

4. Scope

4.1 This policy applies to:

4.1.1 All Institution offices, campuses and learning centres

4.1.2 All students, employees, consultants, contractors, agents and authorized users accessing Institution systems and applications

4.1.3 All Information Technology (IT) systems or applications managed by the Institution that are storing, processing or transmitting information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

5. Definitions

5.1 "Account Lockout Duration" refers to a period of time an account cannot be used after the account lockout threshold has been met.

5.2 "Account Lockout Threshold" refers to how many times an incorrect password can be used before account is automatically disabled.

5.3 "Maximum Password Age" refers to the period of time since a password was set before it is required to be changed.

5.4 "Minimum Password Age" refers to the period of time after changing a password before it can be changed again.

5.5 "Minimum Password Length" refers to the smallest quantity of characters a password can contain to be considered valid.

5.6 "Password" is a code, which, when associated with a user account, provides access to an IT system or application, through an authentication mechanism or a login page.

5.7 "Password History" refers to a user's previous passwords for the specified system.

5.8 "Password Vault" is software used to store and manage passwords securely.

5.9 "Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include: administrative and super user accounts.

5.10 "Security Tokens" are logical codes or physical items that must be used in conjunction with a password to successfully authenticate to an IT system. Examples of a security token include: physical access passes; codes to be used on doors' physical security keypads; PIN codes to be used on smartphones; codes generated by "one-time password" device or software (usually used for two-factor authentication).

5.11 "System or Application Accounts" are user ID's created on IT systems or applications, which are associated with specific access privileges on such systems and applications.

5.12 "Users" are students, employees, consultants, contractors, agents and authorized persons accessing GPRC IT systems and applications.

6. Guiding Principles – Password Protection

6.1 Users must protect passwords at all times against disclosure or unauthorized use, including when generated, distributed, used and stored.

6.2 Passwords must follow a minimum set of security requirements including password length, complexity, reuse, age and account lockout after unsuccessful authentication(s).

6.3 Passwords for Privileged Accounts must follow stronger requirements than regular user passwords.

6.4 In addition to the guiding principles above, passwords must be created and managed in accordance with the guidelines contained in Appendix 1.

7. Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Executive Council	• Approve and formally support this policy.
Vice-President, Administration	• Review and formally support this policy.
Director, Information Technology	• Develop and maintain this policy. • Review and approve any exceptions to the requirements of this policy. • Take proactive steps to reinforce compliance for all stakeholders.
Human Resources	• Present each new employee or contractor with the existing GPRC policies, upon the first day of commencing work with GPRC. • Support all employees and students in the understanding of the requirements of this policy.
Supervisors or Institution Representative	• Support all employees and students in the understanding of the requirements of this policy. • Immediately assess and report to the IT Help Desk any non-compliance instance with this policy.
Contract Administrators	• Ensure that the password responsibilities and obligations of each party to the contractual relationship are outlined in the contract between the Institution and the contractor/sub-contractor.
All users (Employees and contractors, Students, Visitors and/or Volunteers)	• Comply with the requirements of this policy. • Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible.

8. Exceptions to the Policy

8.1 Exceptions to the guiding principles in this policy must be documented and formally approved by the Director, Information Technology.

8.2 Policy exceptions must describe:

8.2.1 The nature of the exception

8.2.2 A reasonable explanation for why the policy exception is required

8.2.3 Any risks created by the policy exception

8.2.4 Evidence of approval by the Director, Information Technology

9. Inquiries

9.1 Inquiries regarding this policy can be directed to the Director, Information Technology.

10. Amendments (Revision History)

10.1 Amendments to this policy will be published from time to time and circulated to the College community.

10.1.1 Post-Implementation Review: Approved May 15, 2018

10.1.2 Reviewed and Approved: March 5, 2019

Appendix 1 - Password Requirements

1. Password Protection

1.1. All access and security codes such as passwords, Personal Identification Numbers ("PINs") and security tokens are considered as confidential information (as defined in the IT Data Classification, Handling Policy) and must be protected and handled accordingly.

1.2. All passwords must be protected at all times, as follows:

1.2.1. Passwords must be memorized and must not be written down.

1.2.2. Passwords must be fully encrypted when they are stored, processed during authentication, or transferred over the network.

1.2.3. When a user needs a new password, it can be transmitted in clear-text over the phone or by email when it is:

- Randomly generated and sent out individually to each user; and
- Valid for a unique transaction, or forced to be changed after the first use.

1.2.4. Passwords can only be stored using an encrypted "password vault" software that has been approved by the Director, Information Technology.

1.2.5. The "Remember This Password" feature in an application (typically within the web browser) must not be used unless the computer is solely used by a single user at all times (i.e. not a shared computer) and its access is protected.

1.2.6. Passwords must be masked when used in an authentication or login window. This includes the system displaying asterisks instead of the actual password characters, as well as the user ensuring no one can read the password as it is entered on the keyboard.

1.3. Passwords used on different systems (i.e. network domain, applications, network devices, and personal passwords) or for different roles and privileges (i.e. regular user, supervisor or administrator) must each be different where possible. Specifically:

1.3.1. The passwords used on GPRC systems must be unique and must not be used on any other non-GPRC systems or applications.

1.3.2. Passwords used to authenticate to external applications, where credentials are sent over an external or public network (for example over the Internet) must be different from passwords used on the internal systems and applications.

1.3.3. The passwords of user accounts with system-level privileges, such as administrator accounts, must be unique and must not be used for other non-administrator accounts.

2. Password Lockout

2.1. The Account Lockout Threshold must be 5 consecutive invalid attempts or less

2.2. The Account Lockout Duration must be a minimum of 10 minutes.

3. Password Complexity

3.1. Passwords must combine a minimum length and the use of complex characters, as follows:

3.1.1. User account passwords should be at least 8 characters long and require the use of at least 3 of the following 4 types of characters:

3.1.1.1. Uppercase characters

3.1.1.2. Lowercase characters

3.1.1.3. Numbers

3.1.1.4. Non-alphabetical characters.

3.1.2. Privileged Accounts, and systems or application accounts (accounts not attributed to a physical person) should be at least 15 characters long and require the use of uppercase and lowercase characters, numbers, as well as non-alphabetical characters (such as punctuation characters, Unicode, or non-printable characters).

3.2. The following words or characters must not be used when selecting a password:

3.2.1. Names such as family names, username, equipment name, make or model

3.2.2. Letters or numbers used in a sequence (including natural or keyboard order) or repeated (1234, 4321, abcde, qwerty, ytrewq, poiuy, zxcvb, aaaaaa, 888888, etc.)

3.2.3. Numerical year or month abbreviations (2013, 2014, jan, feb, mar, apr, etc.)

3.2.4. The words “password”, “iloveyou”, “ilovegprc”, “admin”, “guest”, “trustno1”, and “letmein”.

4. Password Changes

4.1. Passwords for Student accounts do not expire.

4.2. Service and application account passwords that remain static or cannot be changed regularly (e.g. service accounts that are application code dependent) must be documented and be protected with increased access controls.

4.3. New passwords must not be the same as one of the last 10 previously used, must not be based on old passwords, and must sufficiently differ from previously used passwords by changing a minimum of 4 characters.

4.4. Default vendor accounts and passwords (including “public”, “private”, “guest”, “administrator”, “admin”, “system”, or any account that comes pre-configured with a vendor’s solution, application or product) must be changed where possible, before a new system is implemented in production, or within one month after becoming operational.

4.5. New user account passwords must be set up as one time use only (i.e. after generation of a new account password, or when a user has requested a password reset, the user must be required to select a new password after first authentication to the system).

4.6. A verification of the user’s identity must be performed by the IT Director, Help Desk, or designate before granting a new password.

4.7. All passwords associated with a terminated user, including the user's accounts or any shared accounts with administrative or high-level privileges that this user has been exposed to, or that were known to this user, must be immediately reset.

5. Network Domain Passwords

5.1. This section applies to Microsoft Windows network domain and shared folders, desktops, laptops, tablets, servers, and databases, including for the domain and the local password policies. The following domain policy settings must be enforced, as a minimum:

5.1.1. Password history: 10 last passwords used

5.1.2. Maximum password age: 90 days

5.1.3. Minimum Password age: 1 day

5.1.4. Minimum password length:

- 8 characters for regular users
- 15 characters for user accounts with privileges, in order to prevent password attacks based on LM hash

5.1.5. Password must meet complexity requirements: yes

5.1.6. Store passwords using reversible encryption: no

5.1.7. Account lockout duration: 10 minutes

5.1.8. Account lockout threshold: 5 attempts

5.1.9. Reset account lockout counter after: 15 minutes

5.2. Enhanced Network Domain Password Program

5.2.1. Users who take part in IT security awareness training can choose to enhance the security requirements of their domain password.

5.2.1.1. Level 1 – Domain Users who watch at least 10 of the IT Security Awareness videos can choose to have a minimum password length of 10 characters and a maximum password age of 180 days.

5.2.1.2. Level 2 – Domain Users who watch all of the IT Security Awareness videos, and pass a quiz relating to the content of the videos, can choose to have a minimum password length of 15 characters with no maximum password age.

5.2.1.3. Violation of the IT Password Policy will result in suspension from this program for a period of at least two years. During the suspension period, the domain password will be required to be a minimum of 15 characters with a maximum password age of 90 days.

5.2.1.4. Requirements for participation in this program are subject to change.

6. Network Devices Passwords

6.1. This section applies to switches, routers, iLO, Wi-Fi access points, firewalls, load balancers, security devices, etc. The following minimum settings must be enforced:

6.1.1. Password history: 10 last passwords used

6.1.2. Maximum password age: 90 days

6.1.3. Minimum password length: 12 characters where possible (8 characters minimum)

6.1.4. Password must include complex characters (numbers and upper-case letters): yes

6.1.5. Account lockout duration: 10 minutes

6.1.6. Account lockout threshold: 5 attempts

7. Application Passwords

7.1. Application passwords must rely on network domain credentials where possible (Windows Integrated Security).

7.2. When credentials used to authenticate to an application or a system are sent over a public network or an external network (such as the Internet), passwords must be different from the passwords used on the internal network. The following minimum settings must be enforced:

7.2.1. Password history: 10 last passwords used

7.2.2. Maximum password age: 90 days

7.2.3. User account passwords: at least 8 characters long and require the use of uppercase and lowercase characters, as well as numbers

7.2.4. User accounts with privileges, and systems or application accounts (accounts not attributed to a physical person): at least 12 characters long and require the use of both uppercase and lowercase characters, numbers, as well as non-alphabetical characters (such as punctuation characters, Unicode, or non-printable characters)

7.2.5. Account lockout duration: 10 minutes

7.2.6. Account lockout threshold: 5 attempts

7.3. Authentication and encryption libraries that include strong encryption mechanisms must be used to protect passwords.

7.4. Application coding platforms (ColdFusion, Java, .Net, C#, PHP, C++, etc.) as well as any application technology that handle authentication mechanisms or passwords must be updated with the latest available versions and all critical patches released by the vendor.

8. Smartphone Pass-codes

8.1. This section applies to smartphones or cellular phones that process professional email or GPRC information. The following minimum requirements must be enforced:

8.1.1. A pass-code is required to access each device

8.1.2. Pass-codes must be at least 6 characters long

8.1.3. New pass-codes must not be the same as one of the last 10 pass-codes used

8.1.4. Access to the device must be locked after 8 unsuccessful pass-codes entries, for a duration of 5 minutes

8.1.5. Biometric authentication (3D Facial / Iris / Fingerprint) is acceptable as an alternative, or in addition to, a pass-code.

9. Other Passwords

9.1. Voicemail Passwords or Voicemail PINs must:

9.1.1. Have a minimum of 6 numeric digits

9.1.2. Not be the same as the 5 previously used pins

9.1.3. Be locked after 3 incorrect attempts, with a 10 minute wait period

9.2. Remote access passwords used when connecting from an external or public network (such as the Internet) must be:

9.2.1. At least 8 characters long and include uppercase and lowercase characters, as well as numbers

9.2.2. Changed every 90 days when two-factor authentication is not used

9.2.3. Used in combination with a second factor token, where possible

9.2.4. Different from the domain password or any other passwords used within GPRC, where possible

9.3. Pre-shared keys used to connect to Wi-Fi networks must be:

9.3.1. At least 8 characters long and include both uppercase and lowercase characters

9.3.2. Changed regularly

9.3.3. Unique to each Wi-Fi network, where possible

9.4. Using Microsoft Office passwords, PDF creator tools or Winzip / 7zip (with no encryption) is only acceptable for the protection of non-confidential documents (as defined in the IT Data Classification and Handling Policy).