IT Access Control and User Access Management Policy

IT Access Control and User Access Management Policy			
Effective Date	May 20, 2016	**Cross-Reference**	1. Contract Management Policy 2. IT Password Policy 3. Record Classification and Handling Policy
Responsibility	Director, Information Technology		
Approver	Executive Council	**Appendices**	
Policy Review	Every 5 years		

1. Policy Statement

1.1. Protecting access to IT systems and applications is critical to maintain the integrity of the Grande Prairie Regional College ("GPRC", or "the Institution") technology and data and prevent unauthorised access to such resources.

1.2. Access to GPRC systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

2. Background

2.1. Access controls are necessary to ensure only authorized users can obtain access to an Institution's information and systems.

2.2. Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job related duties.

3. Policy Objective

3.1. The objective of this policy is to ensure the Institution has adequate controls to restrict access to systems and data.

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 IT systems and applications.

4.1.3. All IT systems or applications managed by GPRC that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

5. Definitions

5.1. **"**Access Control" is the process that limits and controls access to resources of a computer system.

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

5.3. "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.

5.4. "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.

5.5. **"**Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

5.6. **"**Administrator Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.

5.7. **"**Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.

5.8. "Nominative User Accounts" are user accounts that are named after a person.

5.9. "Non-disclosure Agreement" is a contract between a person and the Institution stating that the person will protect confidential information (as defined in the Record Classification and Handling Policy) covered by the contract, when this person has been exposed to such information.

6. Guiding Principles – General Requirements

6.1. The Institution will provide access privileges to Institution technology (including networks, systems, applications, computers and mobile devices) based on the following principles:

6.1.1. Need to know – users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.

6.1.2. Least privilege – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

6.2. Requests for users' accounts and access privileges must be formally documented and appropriately approved.

6.3. Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the system owner.

6.4. Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.

6.5. Where possible, the Institution will set user accounts to automatically expire at a pre-set date. More specifically,

6.5.1. When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.

6.5.2. User accounts assigned to contractors will be set to expire according to the contract's expiry date.

6.5.3. User accounts will be disabled after 3 months of inactivity. This does not apply to accounts assigned to students.

6.5.4. User accounts with signed contracts for a recurring, continuing, or tenure track appointment for an upcoming term can be active for up to four months between appointments.

6.6. Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access GPRC systems.

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

6.8. Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

6.8.1. An active account assigned to external contractors, vendors or employees that no longer work for the Institution.

6.8.2. An active account with access rights for which the user's role and responsibilities do not require access. For example, users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.

6.8.3. System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.

6.8.4. Unknown active accounts.

6.9. All access requests for system and application accounts and permissions will be documented using the ticketing system in place.

7. Guiding Principles – Privileged Accounts

7.1. A nominative and individual privileged user account must be created for administrator accounts (such as “first_name.last_name.admin”), instead of generic administrator account names.

7.2. Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved.

8. Guiding Principles – Shared User Accounts

8.1. Where possible, the use of specific network domain “security groups” should be used to share common access permissions across many users, instead of shared accounts.

8.2. Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as “guest” and “functional” accounts.

8.3. When shared accounts are required:

8.3.1. Passwords will be stored and handled in accordance with the Password Policy.

8.3.2. The use of shared accounts will be monitored where possible, including the recording of the time of access, the reason for accessing the shared user account, and the individual accessing his account. When the shared user account has administrative privileges, such a procedure is mandatory and access to the monitoring logs must be protected and restricted.

9. Vendor or Default User Accounts

9.1. Where possible, all default user accounts will be disabled or changed. These accounts include “guest”, “temp”, “admin”, “Administrator”, and any other commonly known or used default accounts, as well as related default passwords used by vendors on “commercial off-the shelf” systems and applications.

10. Test Accounts

10.1. Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the IT Director or the IT Help Desk.

10.2. Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.

10.3. Test accounts will be disabled / deleted when they are no longer necessary.

11. Contractors and Vendors

11.1. In accordance with the Contract Management Policy, contracts with contractors / vendors will include specific requirements for the protection of data. In addition, contractor / vendor

representatives will be required to sign a Non-disclosure Agreement ("NDA") prior to obtaining approval to access Institution systems and applications.

11.2. Prior to granting access rights to a contractor / vendor, the IT Director or Help Desk must verify the requirements of Section 11.1 have been complied with.

11.3. The name of the contractor / vendor representative must be communicated to the IT Help Desk at least 2 business days before the person needs access.

11.4. The Institution will maintain a current list of external contractors or vendors having access to GPRC systems.

11.5. The need to terminate the access privileges of the contractor / vendor must be communicated to the IT Help Desk at least 1 business day before the contractor / vendor representative's need for such access ends.

12. Access Control Requirements

12.1. All users must use a unique ID to access GPRC systems and applications. Passwords must be set in accordance with the Password Policy.

12.2. Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.

12.3. Remote access to GPRC systems and applications must use two-factor authentication where possible.

12.4. System and application sessions must automatically lock after 15 minutes of inactivity.

13. Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Executive Council	• Approve and formally support this policy.
Vice President, Administration	• Review and formally support this policy.
IT Director	• Develop and maintain this policy. • Review and approve any exceptions to the requirements of this policy. • Take proactive steps to reinforce compliance of all stakeholders with 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 service desk any non-compliance instance with this policy.

STAKEHOLDER	RESPONSIBILITIES
Contract Administrators	• Ensure that the responsibilities and security obligations of each party to the contractual relationship are outlined in the contract executed between the Institution and the contractor/sub-contractor.
Human Resources	• Present each new employee or contractor with the relevant GPRC IT and Security Policies, upon the first day of commencing work with GPRC. • Support all employees and students in the understanding of the requirements of this policy.
All users (Employees and contractors, Students, Visitors and or Volunteers)	• Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible.

14. Exceptions to the Policy

14.1. Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director.

Policy exceptions must describe:

14.1.1. The nature of the exception

14.1.2. A reasonable explanation for why the policy exception is required

14.1.3. Any risks created by the policy exception

14.1.4. Evidence of approval by the IT Director

15. Inquiries

15.1. Inquiries regarding this policy can be directed to the IT Director.

16. Amendments (Revision History)

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

16.2. Post-Implementation Policy Review Approval: January 29, 2019