IT SECURITY POLICY

IT SECURITY POLICY			
Effective Date	June 27, 2016	**Cross-Reference**	1. IT Security Risk Management Policy 2. IT Operations and Maintenance Policy 3. Records Management Policy 4. Records Classification and Handling Policy 5. IT Access Control and User Access Management Policy 6. IT Continuity and Backups Policy 7. IT Security Incident Management Policy
Policy Holder	Director, Information Technology		
Approver	Executive Council		
Review Schedule	Every 5 years	**Appendices**	1. Network Security Guidelines 2. Anti-Malware Guidelines 3. Data-Centre Security Guidelines 4. Logging and Monitoring Guidelines 5. Security of Third Party Provider(s) Guidelines

1. Policy Statement

1.1 Grande Prairie Regional College ("GPRC" or the "Institution") is committed to protecting IT systems against voluntary or involuntary disruptions or attacks, including protecting its information assets against potential breach, and maintaining data confidentiality, integrity and availability.

2. Background

2.1 Changes to IT systems and data processed or stored by the Institution occur constantly, introducing new threats and vulnerabilities that can be exploited by a malicious user.

2.2 New and disruptive technologies such as smartphones, cloud computing, and social networks, necessitate a new approach to ensure security. At the same time, attackers are more active than ever and use increasingly sophisticated attacks to breach into organizations.

2.3 Implementing a comprehensive set of strong information security controls, processes and practices can reduce these risks.

3. Policy Objective

3.1 The objective of this policy is to define the information security requirements applicable within the Institution to protect IT systems, applications 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 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 “Information Security” is the practice of ensuring that information assets, as well as the technology systems that process, transmit or store such assets, are protected against threats that can affect them. This includes a comprehensive set of controls that cover various factors (human, physical, environmental, and technical) across the lifecycle of information and technology assets, including developing or creating new data or systems, maintaining data and systems, monitoring the use of such assets, detecting and reacting to potential attacks, complying with applicable cyber security and privacy laws and regulations, as well as decommissioning and destroying data and IT systems.

5.2 “Confidentiality” is the status of an information asset, or similarly a technology asset processing such information, relative to the secrecy or privacy of such information (i.e. whether the information asset can be shared with the general public or restricted to only a few authorized persons).

5.3 “Integrity” is the status of an information asset, or similarly a technology asset processing such information, relative to the completeness and unchanged aspect of such information (i.e. whether this information can be modified or not at any time or by any person).

5.4 “Availability” is the status of an information asset, or similarly a technology asset processing such information, relative to availability of access in a timely manner to the asset (i.e. whether this asset needs to be readily accessible at any time or can be accessed after a longer period of time).

5.5 “Users” are students, employees, consultants, contractors, agents and authorized users accessing GPRC IT systems and applications.

6. Guiding Principles

6.1 An evaluation of the Institution security risks must be performed on a regular basis, as per the IT Security Risk Management Policy.

6.2 All information assets must be:

6.2.1. Formally inventoried, following the IT Operations and Maintenance Policy.

6.2.2. Classified and handled in accordance with the Records Classification and Handling Policy.

6.2.3. Monitored, refreshed and replaced to prevent performance issues and the risk of significant breakdown, in accordance with the IT Operations and Maintenance Policy.

6.2.4. Patched regularly to mitigate newly discovered security vulnerabilities, in accordance with the IT Operations and Maintenance Policy.

6.2.5. Protected against external and internal attacks though a combination of anti-malware software, threat detection tools, as well as network segregation.

6.3 Changes to the Institution's technology must follow a controlled procedure, in accordance with the IT Change Management Policy; where relevant, changes related to problems or issues must follow the procedures for handling of IT problems and incidents.

6.4 User accounts, access rights and permissions must be formally controlled by following the IT Access Control and User Access Management Policy.

6.5 User activities and critical IT systems operations must be logged over an appropriate duration to support and enable appropriate investigation requirements. Such activities should be regularly monitored for suspicious activities, network intrusion or wrong-doing.

6.6 Sufficient capabilities must be in place to support business activities in the situation of a disaster or a major disruption of IT systems, following the IT Continuity, Backups, and Recovery Policy.

6.7 Backup systems and processes must be in place, following the IT Continuity, Backups, and Recovery Policy.

6.8 In addition to the guiding principles above, the guidelines contained in the attached appendices must be followed:

6.8.1. Appendix 1 for Network Security

6.8.2. Appendix 2 for Protection Against Malware

6.8.3. Appendix 3 for Data-centre Security

6.8.4. Appendix 4 for Logging and Monitoring

6.8.5. Appendix 5 for Security of Third Party Providers

7. 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. • Take proactive steps to reinforce compliance of all stakeholders with this policy. • Review and approve any exceptions request relative to the requirements in this policy.
Institution Management, Supervisors or Representatives	• Explain the terms of this policy to employees and students and assist users to understand the requirements of this policy. • Ensure that all users follow the requirements of this policy.
Contract Administrators and Managers	• Follow the guidelines provided in this policy when performing due diligence and assessment of the risks related to security for any new contract. • Ensure that responsibilities and 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 existing GPRC policies upon the first day of commencing work with GPRC. • Support all employees and students in the understanding of the policy requirements.
All users (Employees and contractors, Students, Visitors and or Volunteers)	• Comply with the applicable requirements of this policy at all times. • Report all instances of non-compliance 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 IT Director.

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 IT Director

9. Inquiries

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

10. Amendments (Revision History)

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

Appendix 1 - Network Security Guidelines

1. Traffic between the Institution’s network and the Internet must be controlled for:

    1.1. Unauthorized services and ports, using a firewall
    1.2. Potential attacks, using an intrusion detection or prevention capability (IDS/IPS)
    1.3. Malicious code, spam and suspicious traffic, using an anti-malware to inspect malware in emails and other open ports

2. Critical and sensitive application servers, databases and services must not be directly accessible from the Internet. Instead, all traffic must be routed through a Demilitarized Zone (DMZ).

3. Changes to the firewall, IDS/IPS and anti-malware configuration must follow a formal change management process.

4. Where possible, network environments that are accessible to students and / or the public (if applicable) should be segregated from the network zones that are accessible to internal GPRC employees and contractors by a firewall.

5. Wireless network zones intended for students and public use must be segregated from wireless network zones intended for internal GPRC employees and contractors. Access to the GPRC internal Wi-Fi network must be protected using Network Access Control (NAC) authentication.

Appendix 2 - Anti-Malware Guidelines

1. Detection, prevention, and recovery controls to protect against malicious code, along with appropriate user awareness procedures, must be implemented on all:

    1.1. Desktops and laptops
    1.2. Smartphones and tablets, where possible
    1.3. Network servers, where possible
    1.4. Email services

2. Local anti-malware agents or endpoint protection agents must be centrally managed.

3. A central anti-malware or end-point protection management console must be set-up as follows:

    3.1. Anti-malware signatures must always be up to date as soon as new signatures are available.
    3.2. Anti-malware software must be configured to enable real-time scanning and inspection of all incoming or outgoing emails.
    3.3. Automated email alerts must be sent out to an IT person or the Service Desk in the event of an infection or malicious threat.
    3.4. Endpoint devices and servers that cannot be managed by the central anti-malware or end-point protection management console must be equipped with an alternative anti-malware solution.

4. The following events must be reported automatically by email, and subsequently investigated, escalated and remediated in a timely manner:

    4.1. Threat detection
    4.2. Errors with the update of the anti-malware, IDS/IPS signature or software
    4.3. Errors with the installation of an anti-malware agent on a device
    4.4. Changes to the security configuration of the firewall, anti-malware software, end-point protection tool, or IDS/IPS.

Appendix 3 - Data-Centre Security Guidelines

1. The Institution Data Centers (“IDC”) and Satellite Equipment Rooms (“SER”) must be physically protected by perimeter security controls, such as walls running all around and from top to bottom of the area, secure doors and entry gates, or manned reception desks. Doors and entry gates must be locked when reception desks are not manned. Ceiling and floor hatches or tiles must never be left open.

2. Access to the IDC and SER, as well as access to backup media, must be protected by the following controls:

   2.1. Formal authorization for personnel requiring access
   2.2. Escort of all visitors at all times when in secure areas
   2.3. Contactless token, key-card or swipe card attributed uniquely to each authorized user
   2.4. A sign-in/sign-out sheet recording date, time, and object of each access to secure area

3. Authorising access to the IDC/SER:

   3.1. Permanent Key-card/Key Access – Requests must be authorized by the IT Director or its delegate. A form must be filled out with the proper signature and turned in to Information Technology.
   3.2. Contractor Access – Contractors may request a day pass or a contractor key-card. Such requests must be authorized by the IT Director or its delegate. Contractors must sign in and out of the SER/IDC and return the card/key at the end of each visit
   3.3. Guest Access – Guest access to SER/IDC may be allowed in the event of tour or orientation. Guests must be accompanied by an authorized member of IT

4. Environmental controls must be in place to monitor environmental conditions and mitigate:

   4.1. Damage from fire, flood, heat, humidity and vibration (where applicable)
   4.2. Disruptions caused by A/C failure
   4.3. Power failures using Uninterruptable Power Supply (UPS) systems that have sufficient power for a controlled shut-down. For systems where availability is critical, standby generator power sources and UPS systems must have adequate runtime for critical server and network systems operation

5. Environmental and alternative power source controls for IDC and SER must be monitored and alerts actioned on a timely basis.

6. Equipment must be correctly maintained in accordance with vendor recommendations to ensure its continued availability and integrity.

7. Network cabling installation and changes for IDC, SER, and wiring closets must be authorized by the IT department and follow the Network Cabling Procedure & Standards.

8. The following requirements for IDC/SER construction must be observed where possible:

   8.1. Doors must be of steel construction with hinges located inside the room. The lock shall have a steel plate on the outside protecting it from tampering

8.2. Rooms must have environmental controls in place to regulate temperature and humidity

8.3. Sensors with alerting features must be installed to notify staff when temperature exceeds thresholds and when flood conditions occur

8.4. IDC must have a security panel as a second line of access to disable interior alarms

8.5. IDC doorway must be monitored by camera recording on motion

Appendix 4 - Logging and Monitoring Guidelines

1. All critical systems and applications, including GPRC Active Directory (AD) Domain Controllers (DC), applications, servers, databases and network devices must log the following events:

    1.1. Successful and failed logons
    1.2. User account or group creation, change and removal
    1.3. Changes to the auditing / logging policy

2. Audit logs for systems and applications must be stored for a minimum period of 1 year.

3. All security events generated by security tools, such as anti-malware, firewall, IDS/IPS must be recorded for a period of at least 6 months, with a minimum of 1 month available immediately.

4. IT administrators must be alerted when critical system and security events occur on IT systems, network devices and security tools. Security alerts must be properly escalated as per the Security Incident Management Policy.

5. Application owners and IT administrators must review the logs on a regular basis and at least every quarter.

Appendix 5 - Security of Third Party Provider(s) Guidelines

1. Due diligence before contracting or engaging in an agreement with an external party should be performed and should include a review of the provider's:

    1.1. Financial health
    1.2. Reputation
    1.3. Previous or on-going litigations
    1.4. Service and operating capacity, including:

        1.4.1. Technical capacity for professional services
        1.4.2. Experience and credentials of contractor personnel, including professional certifications, technical training and industry experience

    1.5. Security background of its personnel, as appropriate

2. Formal agreements or contracts between the Institution and third party providers should contain the following:

    2.1. Security requirements for confidentiality and privacy
    2.2. Right to audit and / or inspect records and work relating to this agreement or contract
    2.3. Requirement to report any incident immediately
    2.4. Compliance with the Institution's policies and relevant laws and regulations
    2.5. Service deliverables

3. External parties must comply with this IT Security policy at all times when an agreement or contract is active. This covers accessing, processing, communicating or managing GPRC information, as well as performing services or managing products.