IT OPERATIONS AND MAINTENANCE POLICY

IT OPERATIONS AND MAINTENANCE POLICY			
Effective Date	June 27, 2016	**Cross-Reference**	1. Contract Management Policy 2. Fixed Assets Policy 3. IT Continuity, Backup and Recovery Policy 4. Project Management Policy 5. IT Change Management Policy 6. IT Access Control and User Access Management Policy
Policy Holder	Director, Information Technology		
Approver	Executive Council		
Review Schedule	Every 5 years	**Appendices**	1. IT Maintenance Windows Schedule

1. Policy Statement

1.1 Grande Prairie Regional College ("GPRC" or the "Institution") is highly dependent on technology to perform its activities on a daily basis. As a result, the Institution has adopted a formal approach to operating and maintaining its Information Technology ("IT") systems and resources.

2. Background

2.1 Dedicated resources are required to support IT systems in production and ensure effective operations and troubleshooting when necessary. These include:

2.1.1 Sufficient system capacity (processing power, network access and bandwidth, data storage, etc.)

2.1.2 Monitoring procedures to proactively detect system issues or disruptions

2.1.3 Procedures to answer users' service requests, as well as system problems, incidents or disruptions, in a timely manner

2.1.4 Contracts with third party IT service organization(s) where it makes economic sense and allows for efficiencies to address the Institution's needs, compared to using internal resources

2.1.5 Fully trained IT staff

3. Policy Objective

3.1 The objective of this policy is to define the roles, responsibilities and critical elements for the efficient operations and support of IT systems at the Institution.

4. Scope

4.1 This policy applies to:

4.1.1 All Institution offices, campuses and learning centres, including specifically the IT group

4.1.2 All IT systems or applications managed by the Institution that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems

5. Definitions

5.1 "IT Problems" are conditions or situations (known or unknown) that can result in an incident.

5.2 "IT Incidents" are unplanned events which cause an interruption to, or a reduction in, the quality of the IT operations or services.

5.3 "Security Vulnerabilities" are IT problems that present specific risks to cyber security. Vulnerabilities that have a high probability of being exploited and that will highly impact the Institution (risk of operation disruption, data breach, etc.) are often labeled as "Critical" or "High".

6. Guiding Principles – Help Desk and User Support

6.1 The IT Help Desk will act as the central point of contact for all IT technical requests.

6.2 The IT Help Desk will use the following guidelines to prioritize its response to requests:

PRIORITY	CRITERIA	RESPONSE TIME (*)
Urgent	Requests for issues having a significant and immediate impact on the Institution's operations. For example: • An issue affecting all or a large number of users. • An issue preventing users to access critical applications or data, or impacting critical functions (e.g. access to network shares, email, or academic courses). • An information security incident or vulnerability with a critical/high severity/risk. • An issue affecting the ability of a class to be delivered or a meeting to take place. • Other as directed (removal of access rights for an unscheduled terminated user for example).	Within 10 minutes
High	Requests for issues having an important impact on the Institution's operations. For example: • An application error affecting a small group of users. • An issue impacting important functions in a system. • An information security incident or vulnerabilities with a medium/high severity/risk. • Other as directed.	Within 4 hours
Normal	Requests for issues having a limited or non-immediate impact on the Institution's operations. For example: • An issue affecting one person only. • An issue impacting a non-critical function in a system (reporting for example). • A security incident or vulnerability with a low/medium severity/risk. • A question on how to use a non-critical functionality.	Before the end of the next working day
Low	Issues that have no material or immediate impact on the Institution's operations. For example: • A "cosmetic" request, to improve a system functionality "look and feel" or a minor non-functional change to a system.	More than two working days. Within a week if possible.

(*) The response time corresponds to the time to process the request, including analyzing and classifying the request, attributing a ticket to the IT specialist, and dispatching of the IT specialist. This time does not indicate when the ticket must be resolved.

6.3 The assigned IT Staff will respond to all requests submitted to the IT Help Desk within a one-week period where possible. If a request cannot be processed within a one-week timeframe, the IT Staff should inform the user who submitted the request.

7. Guiding Principles – IT Problem and Incident Management

7.1 Where possible, the Institution will take preventative measures to prevent problems from occurring and minimize the impact of incidents that do occur by addressing identified problems as quickly as possible. Examples of preventative measures include the implementation of high-availability and redundant systems and back-up solutions.

7.2 Problems and incidents with a priority of urgent or high must be reported within two hours of detection to contain the issue, and if possible, prevent any further impact.

7.3 GPRC will conduct investigations into problems and incidents with priorities of urgent or high to determine the root cause of the issues, to remediate the issues and return to a normal situation in a timely manner.

7.4 GPRC will communicate with internal and external stakeholders impacted by the problem or incident including students, the public, business partners and law enforcement authorities as required.

7.5 The following key performance indicators and metrics will be used by GPRC to monitor IT problems and incidents:

7.5.1 Number of total problems and incidents by severity (and category where applicable)

7.5.2 Number of problems and incidents resolved

7.5.3 Number of problems and incidents unresolved, with the time since opened and description of why they are still open

7.5.4 Average time to resolve problems and incidents

8. Guiding Principles – IT Asset Management

8.1 The use of non-standard equipment, applications or technology services must be approved by the IT director.

8.2 A list of IT assets will be prepared and maintained in accordance with the Fixed Assets Policy. The following equipment should be included in the list:

8.2.1 Computer and network hardware (desktops, servers, databases and network devices)

8.2.2 Mobile computing devices (smartphones, tablets, laptops, and external hard drives)

8.2.3 Computing storage media (tapes and backups)

8.2.4 Software (applications, software sources and licenses)

8.3 All computer hardware (as defined above) must be tagged by IT for identification and traceability.

8.4 All stakeholders must protect IT assets against the threats of: unauthorized access, theft, loss, or destruction.

8.5 Mobile computing devices (as defined above) must never be left unattended without physical security protection in place, such as: security cable attached to the equipment, locked in a secure cabinet, in a locked office, storage area, or vault

8.6 In addition to preparing and maintaining a list of IT assets per section 8.3, GPRC will document the following information for each IT asset:

8.6.1 Asset description and usage

8.6.2 Level of criticality (High, Medium or Low) for GPRC operations

8.6.3 If the asset processes or stores sensitive information (personal or confidential data)

8.6.4 Status of the IT asset (storage, in use, decommissioned) and location (where possible)

8.6.5 Name of the asset primary user (where applicable)

8.6.6 Name of the asset manager / administrator (where applicable)

8.7 The list of IT assets will be updated whenever an asset's status, location or ownership is changed.

8.8 Before disposing or recycling IT assets, the Institution will ensure all sensitive information is securely and safely removed and record the following information:

8.8.1 Disposal date and time

8.8.2 Method used to remove sensitive data

8.8.3 Status and location of the IT asset after recycling (i.e. asset destroyed, asset sold or given to another organization/entity, etc.)

8.8.4 Name of the person(s) who removed sensitive data and recycled the IT asset

9. Guiding Principles – Systems Replacement

9.1 For IT systems that will no longer be supported by a vendor (including operating systems and application versions), the Institution will upgrade or replace the system at least one year prior to the end of the vendor's support, where possible.

9.2 GPRC will replace IT systems and / or equipment that no longer provide an acceptable level of performance as follows:

9.2.1 Desktops and laptops should be replaced approximately every 5 years

9.2.2 Servers and databases should be upgraded to the latest O/S version every 3 years, where possible

9.2.3 Smartphones should be replaced approximately every 3 years

9.2.4 Commercial applications must be upgraded to the latest version available every 3 to 4 years, at a minimum

10. Guiding Principles – IT Infrastructure and Network

10.1. The Institution will ensure its IT infrastructure availability and performance is continuously monitored (i.e. 24 hours a day, seven days a week). This will include:

10.1.1. Setting up monitoring tools on critical components of the network and systems

10.1.2. Configuring the monitoring tools to ensure that:

10.1.2.1. The appropriate level of information is detected; and

10.1.2.2. Events detected are communicated immediately to the IT Systems team

10.2. Follow section 7 of this policy to react to any network infrastructure availability or performance issue.

10.3. The configuration of systems backups and the recovery processes will follow the IT Continuity, Backup and Recovery Policy.

10.4. The IT Department will be involved in defining the IT technical requirements (i.e. IT and security) for new GPRC projects, including new technology, new or renovated buildings, etc.

10.5. Planned maintenance will occur during the scheduled maintenance window, according to the IT Maintenance Windows Schedule in Appendix 1.

11. Guiding Principles – Vulnerability and Patch Management

11.1 The following activities will be carried out to assist GPRC in the identification of vulnerabilities to systems and applications:

11.1.1 Scanning of web applications that are publicly accessible at a minimum every year

11.1.2 Scanning of web applications that are not publicly accessible at a minimum every two years

11.1.3 Network vulnerability scanning at a minimum every year

11.1.4 Penetration testing, including a detailed review of the system security configuration, at a minimum every five years.

11.2 Identified vulnerabilities must be addressed in a timely manner. Specifically, all critical and high vulnerabilities must be addressed in full within a 30 day maximum period of time, where possible.

11.3 Systems security updates and patches will be applied in a timely manner after they have been published by the vendor. Critical security patches must be applied no later than a month after they have been made available, where possible.

11.4 Patch management, and remediation of identified vulnerabilities, will occur during the scheduled maintenance window, according to the IT Maintenance Windows Schedule in Appendix 1.

12. Guiding Principles – Applications Management

12.1 Only authorized software and licensed products must be used and installed.

12.2 The development of new applications must follow the Project Management Policy (where applicable).

12.3 The purchase of software or commercial off the shelf ("COTS") applications must follow the Purchasing Policy.

12.4 All changes to applications must follow the IT Change Management Policy.

12.5 User access to an application must follow the IT Access Control and User Access Management Policy.

12.6 Planned maintenance will occur during the scheduled maintenance window, according to the IT Maintenance Windows Schedule in Appendix 1.

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. • Communicate with the Institution, directly or through Institution representatives, in informal or formal instances, to understand the Institution needs and expectations, explain the capabilities of the existing technology in production, report on any issues, incidents or disruptions impacting the Institution and how they are addressed, and facilitate the response to any requests from the Institution. • Support Institution representatives in expressing their needs, evaluating and proposing the most efficient solutions, and training users. • Manage IT projects, IT Service delivery, IT operations, IT incidents and IT security. • Ensure any disruption to the technology is addressed in a timely manner. • Report to the Vice President, Administration, the President and CEO as well as the Board of Governors.
IT Infrastructure Team	• Ensure normal operations of the network infrastructure (Network hardware and services). • Ensure normal operations of the data-centre and data-rooms.
IT Applications Team	• Ensure the normal operations and maintenance of the Institution applications. • Assist in the registration of domain names (for websites). • Define the standards and make recommendations on approved development coding standard and libraries. • Ensure security scanning of web applications is performed regularly, and vulnerabilities are addressed in a timely manner. • Communicate with the application owners, the application developers, the IT infrastructure team, and the hosting service company (where applicable), to

	ensure that formal procedures for the development, implementation and changes to applications are followed.
Application Owner	• Define the business needs for the application, including for new applications and changes to existing applications. • Define the level of access for each type of user profile in a formally documented users' authorization matrix. • Review and approve (or modify or reject) user requests related to the application they are responsible for.
Application Administrator	• Implement requests that are approved by the application owner or the IT application team, where applicable. • Monitor the status of the applications they are responsible for. • Maintain the performance level of applications, working as required with the IT application team, or the IT infrastructure team.
Supervisors or Institution representatives	• Review any problem, issue or need from users that cannot be resolved by the standard IT processes for the management of IT problems, incidents, maintenance, support or change. • Contact the IT group for any problem or need that that cannot be resolved by the standard IT processes
Users	• Contact the IT Service Desk for any problem, issue or needs related to the technology. When a problem, issue or needs cannot be addressed by the IT Service Desk, they contact their supervisor or representative • Contact their supervisor or manager for any request related to access rights and privileges, or needs for IT equipment.

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.

14.2 Policy exceptions must describe:

14.2.1 The nature of the exception

14.2.2 A reasonable explanation for why the policy exception is required

14.2.3 Any risks created by the policy exception

14.2.4 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.

Appendix 1 – IT Maintenance Windows Schedule

1. Regular Planned Maintenance and Minor Updates will be scheduled to occur on Thursday Nights. Maintenance may start as early as 6:00 PM, and may run as late as 6:00 AM Friday morning. If possible, disruptive activities will be delayed until after 10:00 PM.

2. Emergency Maintenance and remediation of identified vulnerabilities will occur as soon as possible, and scheduled to reduce impact on operations when possible. Affected users will be notified in advance when possible.

3. Maintenance related to a Project, such as scheduled go-live dates, may occur outside of the regular maintenance window (section 1). Project-related maintenance windows will be scheduled with and approved by the system owners. Affected users will be notified a minimum of one week in advance of the scheduled date.

4. Maintenance in a test environment is considered to be of minimal impact to users and maintenance can be scheduled as needed. Only the affected team or project resources need to be notified.