IT CONTINUITY, BACKUP AND RECOVERY POLICY

IT CONTINUITY, BACKUP AND RECOVERY POLICY			
Effective Date	May 20, 2016	**Cross- Reference**	1. Emergency Response and Business Resumption Policy
Policy Holder	Director, Information Technology		
Approver	Executive Council		
Review Schedule	Every 5 years	**Appendices**	1. IT DRP and Backup Guidelines

1. Policy Statement

1.1. Grande Prairie Regional College ("GPRC" or "the Institution") business operations rely on stable and constantly available Information Technology ("IT") systems. Effective recovery plans are in place to ensure that IT services can be resumed within required recovery times in the event of a system disruption or disaster**.**

2. Background

2.1. A disruption, loss, damage or compromise of IT systems and data may negatively impact GPRC reputation and operations, resulting in significant costs to recover. Formal and comprehensive IT continuity, backup and recovery controls are necessary to mitigate such risks.

3. Policy Objective

3.1. The objective of this policy is to define formal requirements for IT continuity, backup and recovery, in order to prevent or mitigate the risk of IT system disruption or disaster, and allow for an efficient recovery of IT services and data in a timely manner.

4. Scope

4.1. This policy applies to all IT systems or applications managed by GPRC that store, process or transmit information, including network and computer hardware, software and applications.

4.2. This policy does not apply to information that is stored locally by users on desktops, laptops, tablets and mobile phones. Device owners are responsible for appropriate backup of the data stored locally on their mobile devices, with the exception of data synchronized with the device and stored on GPRC servers (such as Outlook emails and contacts).

5. Definitions

5.1. A BCP "Business Continuity Plan" is a comprehensive plan describing the strategy and necessary activities to recover from a significant disruption of business operations, including by relocating part or all personnel and system resources, making urgent decisions, and conducting business operations with diminished or altered capabilities.

5.2. A DRP "Disaster Recovery Plan" is a documented set of procedures describing the key activities that are necessary to recover minimum IT services, applications and data to continue critical business operations, and to fully recover such operations after a disaster affecting normal IT services.

5.3. A RTO "Recovery Time Objective" refers to the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

6. Guiding Principles

6.1. IT systems that are critical to Institution activities must be clearly identified, as well as the potential risks of disruption that apply to them.

6.2. IT continuity, backup and recovery must be managed in accordance with:

6.2.1. The Emergency Response and Business Resumption Policy.

6.2.2. Guidelines contained in Appendix 1 of this policy.

6.3. Recovery Time Objectives ("RTOs") of critical systems must be formally defined as per the business needs.

6.4. Procedures and technology must be in place and tested regularly to ensure:

6.4.1. Prevention against IT system disruption.

6.4.2. Regular and comprehensive backup of critical systems, applications and data.

6.4.3. Timely recovery of critical systems, in line with the business expectation or RTO.

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. • 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, including backup and recovery capabilities.

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 – IT DRP and Backup Guidelines

1. IT Disaster Recovery Plan

1.1. An IT Disaster Recovery Plan (IT DRP) must be formally documented and contain the following details:

1.1.1. Step-by-step procedures to recover critical IT systems and applications and restore data after a major disruption, including:

1.1.1.1. Emergency response to a major disruption

1.1.1.2. Initial recovery of the most critical IT systems

1.1.1.3. Full recovery of most critical systems, applications and data

1.1.1.4. Return to a normal situation

1.1.2. Clear roles and responsibilities.

1.1.3. List of critical systems and applications that are aligned with the BCP.

1.1.4. Detailed minimum requirements and specifications for the critical IT system components, including mapping of critical applications and data hosted on servers.

1.1.5. Salvage list of the most important items to be recovered in an emergency, including the location of the asset (e.g. building, floor, work area and cabinets).

1.1.6. Contact information of key resources, including phone numbers (daytime and non-working hours), email and physical address where possible, for:

1.1.6.1. The IT emergency response team.

1.1.6.2. Other IT contacts (IT staff, 3rd party IT supplier, application vendors, etc.).

1.1.6.3. Other business contacts (applications and system owners and administrators, key suppliers, customers and stakeholders, communication team, etc.).

1.2. The IT DRP plan must be reviewed and tested at least annually to ensure documented information is up to date and that all team members are aware of their responsibilities, roles and tasks to roll-out the plan effectively.

1.3. Regular tests of the IT DRP may include the following:

1.3.1. High-level plan walkthrough

1.3.2. Table top exercise

1.3.3. Simulation exercise

1.3.4. Test of the communication channels and call notification procedures

1.3.5. Data backup restoration

1.4. A copy of the IT DRP plan must be available off-site (using a laptop for example) and in-situ at each data-center.

2. Preventative Requirements

2.1. Protection from power failures or other electrical anomalies must be in place, including where possible:

2.1.1. Multiple power feeds or power supplies.

2.1.2. Uninterruptible Power Supplies (UPS) with sufficient running time for:

2.1.2.1. Switching to an alternative source of power

2.1.2.2. Backing-up IT systems or transferring data

2.1.2.3. Clean shut down of all IT systems. If equipment supporting critical business operations is not capable of auto-shutdown, then the equipment shall be powered down in accordance with an emergency shutdown procedure.

2.1.3. Back-up generators or other source of alternate/secondary power.

2.1.4. All power to critical IT infrastructure shall be filtered to provide a source of “clean” power.

2.1.5. All power supply equipment must be maintained, regularly checked and tested in accordance with the manufacturer’s recommended instructions or procedures.

2.1.6. Surge protection shall be installed, wherever possible, to all buildings housing critical IT processing or infrastructure equipment.

2.2. Protection from environmental hazards must be in place, including where possible:

2.2.1. Hazardous or combustible materials shall not be stored within data-centres or data-rooms.

2.2.2. Appropriate equipment must be installed in data-centres or data-rooms to monitor and react to fire, flood, high temperature, vibration, air quality and dust hazards.

2.3. Systems redundancy and high-availability equipment must be in place where appropriate.

3. Backup Procedures

3.1. Generic backup requirements

3.1.1. Contingency IT equipment must be in place where appropriate.

3.1.2. Backups of critical systems must cover system files, software files and data files, for both the running systems and the default system built image.

3.1.3. A combination of backup technology must be used to ensure the most efficient backup and recovery of operation services. Automated backups must be performed including one of the following solutions:

3.1.3.1. Network-Attached Storage (NAS)

3.1.3.2. Direct-Attached Storage (DAS)

3.1.3.3. Storage Area Network (SAN)

3.1.3.4. Replication and mirroring technologies

3.1.3.5. Backup management system, backup tapes and tape libraries

3.1.4. Different backup media must be used and retained for each backup type (i.e. daily, weekly, monthly, or any other defined period). Further, to ensure greater integrity of the backups, distinct backup media pools must be used where possible.

3.1.5. A Backup Manager must be designated with the responsibility of managing, operating, and troubleshooting backup solutions, as well as answering any requests related to backups and recoveries.

3.1.6. Quality and integrity of backups must be verified at the end of each backup operation.

3.1.7. Backup systems must be configured to automatically generate email alerts, warnings and status updates to the Backup Manager where possible.

3.2. Backup frequency and retention

3.2.1. The following approach, based on a Grandfather-Father-Son (GFS) schedule provides the minimum requirements for the backup of critical IT systems:

3.2.1.1. Daily backups: Differentials or incremental backups.

3.2.1.2. Weekly backups: Full backups.

3.2.1.3. Monthly backups: Full backups.

3.2.2. Daily backups are performed each day. The following backups are performed daily:

3.2.2.1. File-level backups of servers.

3.2.2.2. Recovery-level backups of servers.

3.2.3. Weekly backups are performed each weekend, during non-working hours. The following is performed:

3.2.3.1. File-level backups copied from disk to removable backup tape media.

3.2.3.2. Weekly backup media are stored off-site and retained for a minimum of four weeks.

3.2.4. Monthly backups are performed each month. The following is performed:

3.2.4.1. File-level backups copied from disk to removable backup tape media.

3.2.4.2. Monthly backup media are stored off-site and retained for 3 months.

3.3. Physical security of backup media and contingency IT equipment

3.3.1. Fallback or contingency equipment and backup media stored off-site must be at a sufficient distance to escape any damage from a disaster at the main site.

3.3.2. Long-term storage of backup data must meet the same basic physical and environmental control requirements in place for the critical IT systems in production.

3.3.3. Appropriate care of all backup media must be taken to preserve their integrity. Specifically, tapes must be stored according to the vendor recommendations and must not be exposed to sources of contamination, such as copiers and printers (that emit toner and paper dust), or high voltage electrical equipment (that emit electromagnetic radiation damageable to magnetic tapes).

3.3.4. Backup media reaching the end of their retention period, must be fully erased and recycled in the pool of available backup media.

3.3.5. Any damaged, corrupted or end of life tapes must be destroyed.

3.3.6. All backup media must be labelled and identified with a unique identifier.

3.3.7. A detailed inventory must be maintained at all times to track the position and status of all backup media. The use of an automated inventory system is acceptable but must be completed with regular verification of the true position and status of backup media.

3.3.8. Every physical transfer of backup media off-site must be formally tracked with the following criteria:

3.3.8.1. Date and time of transfer.

3.3.8.2. Origin and destination locations.

3.3.8.3. Name of the person and organization taking the responsibility of the transfer.

3.3.8.4. Detailed inventory of the media being transferred.

3.3.9. Backup media stored off-site must be encrypted; where this is not possible, mitigating controls should be considered.

3.3.10. Security controls must be implemented to prevent access to backup management systems, backup files and backup media, including:

3.3.10.1. Physical and logical access restriction based on the user role and responsibilities.

3.3.10.2. Changing all default login and passwords.

3.3.10.3. Logging of: system access; changes to system configuration, system files and user access rights; and access to the log files.

4. Recovery

4.1. Standard Restoration Process

4.1.1. All restore requests must be formally submitted to the IT Help Desk, who will sequence and address the request to the Backup Manager. Requests must detail the following:

4.1.1.1. Specific file(s) and / or folder(s) that are required to be restored.

4.1.1.2. From which server.

4.1.1.3. From which specific date.

4.1.1.4. To what restore location.

4.1.1.5. Whether the restored data should over-write the current data in the original location or not.

4.1.2. A detailed procedure for data restoration must be documented, including the restoration of data stored in both on-site and off-site backups.

4.2. Emergency Restoration

4.2.1. Emergency restoration must be formally approved by the IT Director.

4.2.2. Due care must be followed to prevent any loss of data or damage to backup media in an emergency.

4.2.3. Details of the backup restoration must be formally documented by the Backup Manager, after the emergency.

5. Roles and Responsibilities - Procedures

Stakeholder	Responsibilities
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, including backup and recovery capabilities. • Formally approve the backup and recovery policy. • Formally approve the IT DRP. • Report to the Vice President, Administration, the President and CEO as well as the Board of Governors.
Backup Manager	• Ensure tools used for backup and recovery are configured as per this Policy. • Ensure backups and recoveries are performed without issue and remediate any such issue. • Answer and address requests to backup or to restore backed-up data or systems. • Provide recommendations regarding the processes to backup and recover IT systems, applications and data, and participate in the development of the BCP and the IT DRP. • Provide recommendations to improve or update this Policy.
Systems owners	• Identify the critical IT systems, applications and data necessary to support critical business operations. • Define the minimum availability requirements for their systems, including Recovery Time Objectives (RTOs). • Participate in the development of the BCP and the IT DRP.
Supervisors or Institution representatives	• Participate in the development of the BCP and the IT DRP. • Communicate with the IT group for any need, concern or question related to IT systems availability, IT backup and recovery services.
Users	• Contact the Help Desk for any question or concern related to the technology. When a question or concern cannot be addressed by the Service Desk, contact their supervisor or representative. • Backup their personal files stored locally on computers and mobile devices.