A-27 Preparedness Planning – Information Technology

Preamble: The primary objective of the Preparedness Planning-Information Technology Policy is to protect the organization in the event that all or part of its operations and/or computer services are rendered unusable.

The plan should minimize disruption of operation and ensure some level of organizational stability and an orderly recovery after a disaster.

Policy: Management personnel are responsible for protecting all assets of the organization. These assets include employees, physical property, information and records relating to the conduct of business. This policy specifically addresses information technology systems and records management.

Authority

The decision to implement Preparedness Planning procedures is the responsibility of the CAO or designate. The Preparedness Planning Team (the Team) will convene as soon as possible after a disaster has occurred to assess damages and make recommendations to the CAO.

Distribution

This plan will be distributed to and used by those persons responsible for its implementation and operation. These individuals, the Team, are identified in Appendix A. Appendices will be maintained and updated by the Administrative Assistant whenever significant changes occur.

Basic Recovery Plan Requirements

The basic requirements for the Recovery plan are as follows:

- Preparedness Planning Team
- Preparedness Planning documentation backup
- Backup computer facilities
- Recovery Plans

Disaster Recovery Team

Team members are specifically responsible for:

- Identifying and protecting all assets within their assigned area of control.
- Understanding their obligation to protect the organization's assets.
- Developing, coordinating, testing and maintaining it by keeping the information it contains current.
- Being familiar with the Plan and understanding their part in the recovery effort.
- Reducing potential risks by implementing any monitoring established security measures and procedures and initiating corrective action when violations are observed.
- Ensuring that the procedures set forth in the Plan are properly executed in the event of a disaster.

The Team will be responsible for one or more of the following functions.

- Recovery Electronic Data administration
- Insurance notification
- Supplies
- Systems software
- Application software
- Facilities

- Hardware
- Communications
- Operations

In the event of a disaster or major failure, the Team will convene with as many Team members as possible. All members of the Team will assess damage to computer facilities, control and coordinate recovery/backup actions and make recommendations to the CAO.

Preparedness Planning Documentation

Inventory Necessary Office Equipment

- Desk and chair
- Computer
- Computer software
- Telephone
- Calculator

Catalog of Supporting Equipment

- Servers
- Server Software
- Data backups
- Phone System

Insurance and Budget

- The Chief Financial Office will review insurance coverage.
- The Annual budget will be the loss deductible of $1,500.

Backup computer facilities

Offsite storage of data files backup

In the event that disaster occurs, having backup stored off site is critical. Appendix F defines the backup schedule. Offsite backup of server to an external storage device is done daily and stored offsite with the Administrative Assistant or designate.

Backup facilities

In the case of fire or natural disaster it may become necessary to move/relocate the office to a backup location. The location currently designated is the airport satellite office in the hangar.

Recovery Plans

Preparedness Planning

This section outlines the minimum steps required to ensure the CCRD can fully recover from a disaster.

1. The Preparedness Plan must be kept current, and all of the Team members must be made aware of any changes.
2. A copy of the Preparedness Plan is stored offsite in the CCRD safety deposit box at the Williams Lake and District Credit Union Bella Coola Branch.
3. All Team members should be aware of the consequences of a disaster and what they can do while recovery is in progress.
4. Procedures and lead times for replacement equipment and communications should be established.

In the event that there is warning of an impending disaster, (e.g. potential flood situations, fire or potential building damage) the following steps should be taken:

1. Notice should be given to as many Team members as possible.
2. The CAO should be briefed and a decision should be made whether to shut down the systems.
3. The Team should convene and review whatever actions may be necessary.

Emergency Response

This section details the basic actions to be taken in the event of a disaster situation.

1. The CAO or assignee will be notified as soon as possible.
2. The Team will be notified and assembled as soon as reasonable under the circumstances.
3. Team members will assess damages to their individual areas of expertise.
4. Team members will advise the CAO as to the extent of damage and recovery procedures necessary so that the decision to move the office can be made after the assessment of damage done to the current office.
5. Pertinent vendors will be contacted and negotiations will be made for the delivery of equipment. Delivery time will be noted.
6. All Team members will be given an estimated time to return to either full or degraded service.
7. Each Team member will supervise their own area of expertise.
8. Computer facilities will be secured.

Recovery Procedures

If it is decided to transfer the office and computers to the off site location:

- It is assumed that the basic emergency procedures have been followed as detailed in Recovery Plans
- An inventory of the status of existing equipment and files will be compiled
- Initiate the recovery site.
- An estimated time of delivery of computers and equipment will be established
- Systems will be tested and loaded as soon as the vendors release them to the CCRD

Recovery Timetable

The following timetable does not take into account the amount of time required to re-input data which may have been lost during recovery period.

Day 1	Convene the Preparedness Planning Team and assess damages. Contact vendors to replace needed equipment.
	If able restore programs and data, test integrity of programs and data. Begin restoring communications and networking capabilities.
Day 2	Restore operations to priority departments
	Determine priority of data processing
Day 4	Delivery and setup new equipment. Restore full communications and networking capabilities

Preparedness Planning Review

The Preparedness Planning Team will convene annually to review the Plan and Appendices. Updates or revisions will be made at this time.