



D M G M C

ADM(Mat)

EMERGENCY

BUSINESS CONTINUITY PLAN

[ADM(Mat) EBCP]

DRAFT v1.0

(Intentionally Blank)

RECORD OF CHANGES

(Intentionally Blank)

TABLE OF CONTENTS

1. Introduction.....	7
1.1 Background.....	7
1.2 Introduction to this document.....	7

1.3	How to use this document.....	7
1.3.1	Part Contents.....	7
1.4	Audience.....	7
1.5	Distribution.....	8
2.	Introduction to the Plan.....	9
2.1	Purpose.....	9
2.2	Scope.....	9
3.	Plan Design.....	10
3.1	Assumptions.....	10
3.2	Maintenance of Business Continuity Plans.....	10
3.3	Testing of Business Continuity Plans.....	11
3.4	Business Continuity Teams and Responsibilities.....	11
3.4.1	DND/CF BCP Team.....	11
3.4.2	Business Continuity Management Team.....	11
3.4.3	Operations Team.....	12
3.4.4	Networks Team.....	13
3.4.5	Accommodations Team.....	13
3.4.6	Communications Team.....	13
3.4.7	Transportation Team.....	14
3.4.8	Influenza Pandemic Team.....	14
4.	Disaster Response.....	15
4.1	What to do in the Event of a Disaster.....	15
4.1.1	Standard Emergency Procedures.....	15
4.2	Recovery Scenarios.....	15
4.2.1	Scenario one: Minor Damage.....	15
4.2.2	Scenario two: Major Damage.....	16
4.3	Standard Operating Procedures.....	17
4.3.1	Business Continuity Management Team.....	17
4.3.2	Operations Team.....	17
4.3.3	Networks Team.....	18
4.3.4	Accommodations Team.....	19
4.3.5	Communications Team.....	20
4.4	Command Center.....	21
4.4.1	Primary Command Centre.....	21
4.4.2	Alternate Command Centre.....	21
4.4.3	Command Center Requirements.....	21
4.5	Standby Facility.....	22
4.5.1	Location.....	22
5.	Influenza Pandemic Response.....	23
5.1	In the Event of an Influenza Pandemic.....	23
ANNEX A: ADM(Mat) BCP GOVERNANCE STRUCTURE AND CONTACTS.....		25
ANNEX B: FAN-OUT CONTACT LIST.....		27
ANNEX C: DIVISIONAL INFORMATION AND CRITICAL BUSINESS FUNCTION.....		28
ANNEX D: EMERGENCY CONTACTS.....		29
ANNEX E: OTHER CONTACTS.....		30
ANNEX F: PLANS DISTRIBUTION LIST.....		31
ANNEX G: 76 COMM GP INCIDENT SERVICE RESPONSE TARGETS.....		32
ANNEX H: ADM(Mat) PERSONNEL CONTACT LIST (NCR).....		33

(Intentionally Blank)

1 Introduction

This section contains information about this document, which provides the written record of the ADM(Mat) Emergency Business Continuity Plans (EBCP).

1.1 Background

In response to incidents such as the terrorist attacks in the United States on 11 September 2001, the 1998 ice storm, the 2004 widespread power outage and the impending threat of pandemic influenza, the Treasury Board Secretariat (TBS) recognized the need to establish a comprehensive process to ensure the Continuity of Constitutional Government and the continuity of critical government services in the face of man made or natural disaster. The effects of any one of these events could be significant and underscores the requirement for all departments. The TBS developed the Business Continuity Planning Program and mandated its implementation through the Government Security Policy.

The time required to produce a concrete Business Continuity Plan for the size of ADM(Mat)'s organization would take much time and effort. It's estimated to take anywhere from 1 to 2 years. In the event of a disruption or a disaster that could occur tomorrow there is a need to produce a "quick" Business Continuity Plan to provide guidance on how to deal with the disruption and minimize downtime of the organizations critical services in a rapid and efficient matter. As a result, ADM(Mat)'s Emergency Business Continuity Plans (ADM(Mat) EBCP) was produced to address this problem. As we progress forward in the development of ADM(Mat)'s BCP, the EBCP will be updated simultaneously.

1.2 Introduction to this Document

This document is intended to assist the Government in ensuring the health, security and economic well being of Canadians by means of plans and procedures for ensuring the continuity of critical government services, known as business continuity plans. Planning for the business continuity within ADM(Mat) in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disruption of a disaster affecting the Group's services, information systems, it's infrastructure, and it's personnel, requires the cooperative efforts of many support organizations. This plan describes, outlines and coordinates the efforts required for business continuity within ADM(Mat). Please note, this document does not contain the Disaster Recovery Procedures for ADM(Mat)'s information systems, this is ADM (IM)'s area of responsibility.

1.3 How to use this Document

Use this document to learn about the issues involved in planning for the continuity of the critical and essential business functions for the Materiel Group, as a checklist of preparation tasks, for training personnel, and for recovering from a disaster. This document is divided into four parts, as described below.

1.3.1 *Part Contents*

- Information about the document itself.
- Design of the Plan that this document records, including information about the overall structure of business continuity planning within the Materiel Group.
- The function and responsibilities of the individual disaster response teams.
- Recovery actions for the disaster response teams and important checklists such as the notification list for a disaster and an inventory of resources required for the environment.

1.4 Audience

This document addresses several groups within the Group's administration structure with differing levels and types of responsibilities for business continuity, as follows:

- DND/CF BCP Team.
- ADM (Mat) Business Continuity Management Team.
- Operations Team.
- Accommodations Team
- Communications Team
- Transportation Team

It should be emphasized that this document is addressed particularly to the members of ADM(Mat)'s Business Continuity Management Team, since it has the responsibility of preparing for, responding to, and recovering from any disaster that impacts the Group.

1.5 Distribution

As the written record of the Group's Business Continuity Plan, this document is distributed to each member of the Business Continuity Management Team, and also to members of the other disaster response teams.

It is also distributed to members of the divisional OPIs, information systems management and others not primarily involved with the direct recovery effort (e.g., DND/CD BCP Team, DPM Secur 4, CFSU(O), ADM(IM), and other DND disaster response teams) for their personal reference and because they may be involved indirectly with continuity efforts within the Materiel Group.

2 Introduction of the Plan

For the purposes of this document, the term disaster will be used to represent natural disasters, human-made disasters, and disruptions.

2.1 Purpose

The purpose of ADM(Mat)'s EBCP is to:

- Provide directions and procedures to ensure the continuance of the groups critical operations.

-

Reduce and mitigate the impacts of a disaster.

The Materiel Group increasingly depends upon its facilities, personnel, equipment and inventory on computer-supported information processing and telecommunications. This dependency on information systems will continue to grow.

The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall ability of the Group to provide essential services.

Group management recognizes the low probability of severe damage to its facilities, personnel and information processing services capabilities that support the Group. Nevertheless, due to the potential impact to the Group, a plan for reducing the risk of damage from a disaster and for maintaining the business services, however unlikely, is vital. The Group's Business Continuity Plan is designed to reduce the risk to an acceptable level by ensuring the restoration of High priority assets quickly, and all Medium and Low priority assets in a timely manner.

The Plan identifies the critical functions of the Group and the resources required to support them. The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and response, and that the proper steps will be carried out to permit the timely restoration of services.

The BCP also specifies the responsibilities of the Business Continuity Management Team, whose mission is to establish procedures to ensure the continuity of divisional business functions. In the event of a disaster affecting any of the functional areas, the Business Continuity Management Team serves as liaison between the functional area(s) affected and other Level 1 organizations providing major services and to the Departmental level. These services include the support provided by CFSU, security, and public information dissemination among others.

The Group is indirectly involved in any disaster impacting the facilities. A disaster of this magnitude is one that would affect other groups and commands within DND for this reason, the DND/CF BCP takes precedence in any disaster event affecting more than the Group itself.

2.2 Scope

Although ADM (Mat) has presence Nationally, the focus of this Plan is limited to the National Capital Region (NCR). The facilities housing the personnel of the Materiel Group within the National Capital Region, Pearkes Building, Louis St-Laurent Building, West Memorial, National Printing Bureau, Cumberland Building, Woodline, Uplands, and Coinomatic. The implementation tasks associated with the NCR would be consistently applied to regionalized support to the Canadian Forces (CF) presence in each region and the senior on-site Manager would take the leading role. The Commanding Officer in each region would handle the regional security requirements. However Director General (DG's) are responsible to ensure that their field units have a BCP agreement in place with their host units. It is recommended that the Divisions periodically review their field units BCP agreement.

3 Plan Design

This section, Part 3, describes the philosophy of business continuity planning within the Materiel Group generally, and an overview of the functions of all disaster response teams in implementing this Plan.

3.1 Assumptions

This project is focused on business resumption in case of a temporary or extended loss of one or more assets due to a disaster. It does not include the physical or electronic security of the assets. The assets include facilities, equipment, personnel and information. The BCP will include business continuity activities within the Materiel Group necessary to support ongoing military operations.

In the event of business interruption or disaster, it is assumed that:

- ADM (Mat) services would continue, but in a limited capacity focusing on the situation at hand.
- ADM (Mat) will ensure that funding will be available to meet all requirements to achieve the BCP.
- ADM(Mat) Divisions will create Standard Operational Procedures (SOPs) to ensure that Divisional staff understand their responsibilities when the BCP is activated.
- Critical services are defined, and that a list of these services are provided to the Divisions.
- Each Division assigns an OPI who understands the "business" of the Division, will co-ordinate the Divisional response, and represent the Division at BCP meetings.
- TBS will provide additional direction concerning security and attendance of government employees in an increased threat environment.
- CFSU (O) will provide timely communication and support in the management and co-ordination of safety/security issues.
- CFSU (O) will have a process to ensure food, water and cots are available to meet the requirements of staff who are employed within ADM(Mat) locations throughout to NCR.
- City of Ottawa has contingency plans for public transit system; policing, emergency response to aid government workers leaving the downtown core if a large-scale evacuation is required.

Be advised that in the event of a major crisis all resources will be stretched to the limit and large portions of the infrastructure may not be available for use. In the event of an evacuation of government buildings, public transit may not be available to relocate employees, heavy traffic jams may inhibit commuting and phone systems, including cellular, may be flooded.

3.2 Maintenance of Business Continuity Plan

Ensuring that the Plan reflects ongoing changes to resources is crucial. These tasks include updating the Plan and revising this document to reflect updates, testing the updated Plan, and training personnel. The coordinator of the Business Continuity Management Team is responsible for this comprehensive maintenance task.

Quarterly, the Business Continuity Management Team Coordinator ensures that the Plan undergoes a more formal review to confirm the incorporation of all changes during the prior quarter. Annually, the Business Continuity Management Team Coordinator initiates a complete review of the Plan, which could result in major revisions to this document. These revisions will be distributed to all authorized personnel, who exchange their old plans for the newly revised plans. At that time the Coordinator will provide an annual status report on continuity planning to the Business Continuity Management Team and to the VCDS, who is responsible for business continuity planning for DND/CF as a whole.

3.3 Testing of Business Continuity Plan

Testing the Business Continuity Plan is an essential element of preparedness. Partial tests of individual components and recovery plans of specific functional areas and disaster response teams should be carried out on a regular basis by Group personnel. A comprehensive exercise of the Group's continuity capabilities and support of designated recovery facilities should be performed on an annual basis by Group personnel.

There are three levels of testing involved in maintaining this plan. They are:

Desktop or checklist tests (Table Top). This involves the members of the teams evaluating the plan by checking off the various components of the plan to ensure that nothing has changed. If changes have occurred, the plan should be updated to reflect those changes. In addition, the changes should be distributed to everyone on the distribution list. The desktop test should occur 2-4 times per year.

Simulations. A simulation involves an actual run-through of the plan procedures in a situation similar to a fire drill. Participants perform the actual steps described in the procedures. However, the actual production environment continues to run and, therefore,

there is no affect on normal operations. For simulations, it is necessary to have a backup site that can be used to evaluate the recovery procedures for information processing. Simulations should be run annually.

Live exercise. A live exercise is one in which the production environment is stopped without warning anyone not involved in the planning of the exercise. All steps from the initial "discovery of a problem" to the complete recovery of the production environment must be performed. This exercise must be planned well to ensure minimal impact on the overall operations of the Group. A live exercise should be completed every 2-5 years.

The desktop or checklist tests should evaluate the entire plan, including the plans of all disaster response teams. Simulations and live exercises can be planned to evaluate all or parts of the overall continuity plan.

3.4 Recovery Teams and Responsibilities

The organizational backbone of business continuity planning within the Group is the Business Continuity Management Team. In the event of a disaster affecting the services or resources of the Group, the Business Continuity Management Team will respond in accordance with this Plan and will initiate specific actions for service restoration. The DND Business Continuity Management Team, other Level 1 Business Continuity Management Teams, the Disaster Recovery Management Team, and the Public Relations Team are called into action as necessary under the authority of the DND Oversight Team, which has the responsibility for approving all business continuity and disaster recovery actions within the Department.

The following are the roles and responsibilities to be used in the event of an emergency and does not reflect the current organizational structure within the Materiel Group or within DND. Both DND and ADM(IM) must take prime responsibility for the disaster recovery activities and providing support to the Materiel Group. The Group is responsible for all business continuity activities within its mandate and focuses mainly on the restoration of information services, not IT services. The Group will also provide representatives for the Damage Assessment and Salvage Team so that damage to Group assets can be evaluated and salvaged if possible.

3.4.1 DND/CF BCP Team

The DND BCP Team has the responsibility for giving directions and approving actions regarding business continuity and disaster recovery within the DND/CF. It ensures that all governmental and departmental policies are followed. When necessary, the team coordinates all disaster recovery and business continuity activities for the department. This team is the one that declares a disaster situation. This team oversees the development, maintenance and testing of disaster recovery and business continuity plans addressing all Level 1 critical business functions within the Department.

3.4.2 Business Continuity Management Team

The Business Continuity Management Team is responsible for providing overall direction of the recovery operations. It ascertains the extent of the damage, activates the recovery organization and notifies the team leaders. Its prime role is to monitor and direct the recovery effort. It has a dual structure in that its members include Team Leaders of other teams.

The Business Continuity Management Team Leader is responsible for deciding whether or not the situation warrants the activation of disaster recovery procedures. If he decides that it does, then the organization defined in this section comes into force and, for the duration of the disaster, supersedes any current management structures.

The Business Continuity Management Team operates from the Command Centre.

Responsibilities:

- Managing all the recovery teams and liaising with Materiel Group's management, Director Generals, managers and users, as appropriate.
- Evaluating the extent of the problem and potential consequences.
- Notifying senior management of the disaster, recovery progress and problems.
- Initiating disaster recovery procedures.
- Coordinating recovery operations
- Liaising and working with the other Group Principal and Environmental Command disaster management teams who may be also affected by the disaster.
- Monitoring recovery operations and ensuring that the schedule is met.

- Documenting recovery operations.
- Expediting authorization of expenditures by other teams.
- Recording emergency extraordinary costs and expenditure.
- Making a detailed accounting of the damage.
- Ensuring that the conversion to the standby facilities and final resumption of operations at the data centre are under sufficient audit control. This will provide reliability and consistency to the accounting records.
- Ensuring that appropriate arrangements are made to restore the site and return to the status quo within the time limits allowed for emergency mode processing.
- Approving the results of audit tests on the critical applications, which are processed at the standby facility shortly after they have been produced.
- Declaring that the Business Continuity recovery plan is no longer in effect.

3.4.3 Operations Team

The Operations Team is responsible for the IS environment (server room and other vital IS) and for performing tasks within those environments. This team is responsible for restoring IS processing and for performing server room activities.

Responsibilities:

- Ensuring that the standby equipment meets the recovery schedules.
- Installing the computer hardware and setting up the latest version of the operating system at the standby facility.
- Obtaining all appropriate historical/current data from the offsite backup location and restoring an up-to-date application systems environment.
- Providing the appropriate management and staffing of the standby IS site, in order to meet the defined level of user requirements.
- Support operable versions of all critical applications needed to satisfy the minimum operating requirements.
- Performing backup activities at the standby site.
- Providing on-going technical support at the standby facility.
- Working with the Networks Team to restore local and wide area data communications services to meet the minimum processing requirements.
- Obtaining all necessary back-ups from off-site storage.
- Initiating operations at the standby facility.
- Re-establishing software libraries and databases to the latest backup.
- Coordinating the user groups to aid the recovery of any non-recoverable data
- Providing sufficient personnel to support operations at the standby facility
- Managing the standby facilities to meet users' requirements
- Establishing processing schedule and informing user contacts
- Arranging for acquisition and/or availability of necessary computer supplies
- Ensuring that all documentation for standards, operations, vital records maintenance, application programs etc. are stored in a secure/safe environment and reassembled at the standby facilities, as appropriate

3.4.4 Networks Team

The networks team (*ADM (IM)*) is responsible for all IS networking and communications.

Responsibilities:

- Arranging new local and wide area data communications facilities and a communications network, which links the standby facility to the critical users
- Installing a minimum voice network to enable those identified as critical telephone users to link to the public network.

- Evaluate the extent of damage to the voice and data network and discuss alternate communications arrangements with telecom service providers.
- Establish the network at the standby facilities in order to bring up the required operations.
- Define the priorities for restoring the network in the user areas.
- Order the voice/data communications and equipment as required.
- Supervise the line and equipment installation for the new network.
- Providing necessary network documentation.
- Providing ongoing support of the networks at the standby facility.
- Re-establish the networks at the primary site when the post disaster restoration is complete.

3.4.5 Accommodations Team

The Accommodations Team is responsible for finding and preparing appropriate temporary accommodations for personnel and equipment to ensure that the impact of the disaster situation on business continuity activities is minimized. This may include the acquisition of new facilities or the sharing of existing facilities.

Responsibilities:

- Administering the reconstruction of the original site for recovery and operation
- Arranging all transport to the standby facility.
- Controlling security at the standby facility and the damaged site.
- In conjunction with the Business Continuity Management Team, evaluating the damage and identifying equipment which can be salvaged.
- Working with the Networking Team to have lines ready for rapid activation.
- Ensuring that arrangements are appropriate for the prevailing circumstances (i.e. any replacement equipment is immediately available etc.)
- Preparing the original data centre for re-occupation.
- Arranging for all necessary office support services.
- Dealing with staff safety and welfare.

3.4.6 Communications Team

The Communications Team is responsible for obtaining communications directives from the Business Continuity Management Team, and communicating information during the disaster and restoration phases to employees, suppliers, customers and the media.

Responsibilities:

- Liaising with the Business Continuity Management Team to obtain directives on the messages to communicate.
- Informing suppliers and customers of any potential delays.
- Informing employees and union representatives of the recovery progress of the schedules.
- Ensuring that there is no miss-communication that could damage the image of the department.
- Any other public relations.

3.4.7 Transportation Team

The Transportation Team, a temporary team, is responsible for transporting personnel, equipment, and materials to the back-up locations as necessary.

Responsibilities:

- Liaising with DND Transportation and Accommodations Team to coordinate the transportation of personnel and equipment.

3.4.8 Influenza Pandemic Team

The Influenza Pandemic Team is responsible for the distribution of Pandemic Influenza packages, posters, and pamphlets to mitigate influenza transmission, and to manage, evaluate, and take care of personnel who are ill or suspect to be ill.

Responsibilities:

- Liaising with the Business Continuity Management Team to obtain directives on the messages to communicate.
- Liaising with PMed and PWGSC on medical supply stockpiles and potential need for sources of additional supplies
- Liaising with PMed and PWGSC for Vaccine distribution.
- Monitor staff who are ill or suspected to be ill.
- Contact staff who are unexpectedly absent from work.
- Ensures workplace has adequate supplies of:
 - i. Medical Supplies
 - ii. Hand Hygiene Products.
 - iii. Cleaning Supplies.
 - iv. Mask.
- Help Influenza Manager to monitor staff who are ill or suspected to be ill.
- Manage, evaluate and take care of staff who have fallen extremely ill.

4 Disaster Response

4.1 What to do in the event of a disaster

The most critical and complex part of managing resources is in the planning and organization of the required personnel during the invocation of the plan. Funding must be available in the event of a disaster.

Personnel must be well rehearsed, and familiar with the disaster recovery plan and be sure of their assignments.\

4.1.1 Standard Emergency Procedures

The first priority in a disaster situation is to ensure safe evacuation of all personnel.

In the event of a major physical disruption, standard emergency procedures must be followed. This means immediately:

- Activating the standard alarm procedures for that section of the building to ensure that Medical, Security and Safety departments and emergency authorities are correctly alerted.
- If necessary, evacuating the premises following the laid down evacuation procedures and assembling outside at the designated location, if it is safe to do so.

The First Steps for the Recovery Teams

The

Facilities Team assesses the nature and extent of the problem.

If it is safe to do so, the Operations Team switches off all equipment in the server room.

Building Security alerts the *Disaster Management Team Leader*.

The Facilities Team give an initial assessment to the *Disaster Management Team Leader*, who needs to know the extent of the damage to the buildings and equipment and the staff status. Also report what actions have been taken.

The Next Steps

The Business Continuity Management Team Leader decides whether to activate the BCP plan, and which recovery scenario will be followed.

The recovery teams then follow the defined recovery activities and act within the responsibilities of each team, as defined in this disaster recovery plan.

4.2 Recovery Scenarios

This section describes the various recovery scenarios that can be implemented, depending on the nature of the disaster and the extent of the damage. The *Disaster Management Team Leader* decides which recovery scenario to implement when he or she activates the disaster recovery plan.

4.2.1 Scenario One: Minor Damage

In this scenario, only a part of the IS environment is out of action, but the communication lines and network are still up and running. The goal of the recovery process in this case is to move the applications from the systems, which are unavailable to the Standby Facility.

In this scenario the building is still available and the users can use normal office space to wait for the restart of computer processing.

Action Plan

Task	Team
Evaluate the damage	BCP Management Team / PWGSC Disaster Management Facilities and Operations
Identify the concerned applications	BCP Management Team
Request the appropriate resources at the Standby Facility	BCP Management Team/ Accommodations Team
Request Systems staff support from 76 CommGp (ITSS)	Operations Team
Obtain the appropriate backups	Operations Team
Restart the appropriate applications at the Standby Facility	Operations Team
Inform users of the new procedures	Communications Team
Order replacement equipment to replace the damaged computers.	Operations Team
Install replacement equipment and restart the applications	Operations Team
Inform users of normal operations	Communications Team

4.2.2 Scenario two: Major Damage

In this scenario, the entire IS environment (or most of it) is out of action. Communication lines and the network are out of action.

The goal of the recovery process in this scenario is to move all identified applications to the Standby Facility.

This scenario requires a full recovery procedure, as documented in this disaster recovery plan.

Action Plan

Task	Team
Emergency planning meeting to receive direction from Senior management	BCP Management Team
Staff the Command Centre, issue order that ADM(Mat) is on DR Mode	BCP Management Team
Review DR plan and initiate action items	BCP Management Team, Operations Team, Facilities Team, Communications Team, Networks Team.
Contact 76 CommGp and request ITSS support	Operations Team
Prepare the Standby Facility for operations	Operations Team, Accommodations Teams, Networks Team
Restart the appropriate applications at the Standby Facility	Operations Team
Inform users of the new procedures	Communications Team
Order replacement equipment to replace the damaged computers.	Operations Team
Install replacement equipment and restart the applications	Operations Team
Inform users of normal operations	Communications Team

4. 3 Standard Operating Procedures

4.3.1 *Business Continuity Management Team*

Immediate

1. Receive an initial assessment of the nature and extent of the problem.
2. Decide whether to activate the Plan.
3. Alert all Recovery team leaders.
4. Alert and mobilize all other team members.
5. Make a preliminary (verbal) report to senior management.
6. Call an initial meeting of the recovery team leaders with the following objectives:
 - To define the problem, the extent of the disruption, determine consequences and the probable implications for the foreseeable future.
 - To set up a specified location as a Command Centre.
 - To agree each team's objectives for the next three hours (suggested timings).
 - To set up a second meeting for three hours later (suggested timings).
7. Make a second, more detailed, report to senior management on the content of the meeting and the actions being taken.

Within Three Hours

8. Call a second meeting of the recovery team leaders with the following objectives:
 - To receive initial reports from the recovery team leaders.
 - To take the decision to implement disaster recovery procedures.
 - To agree each team's objectives for the next twenty-four hours.
 - To set up a third meeting for twenty-four hours later.

Within Twenty Four Hours

9. Contact the standby facilities to invoke the installation.
10. Agree installation schedule with the standby facility.
11. Prepare plans for the transition to the standby facility.
12. Make official declarations (for example, place of work change to any regulatory authorities).
13. Report progress to senior management.

Ongoing

14. Act as the main point of contact with the emergency services.
15. Monitor on a regular basis all activities to exercise and maintain control over delivery and installation dates.
16. Document progress against agreed schedules.

4.3.2 *Operations Team*

Immediate

1. Attend the initial meeting called for recovery team leaders.
2. Alert and mobilize all other team members.

Within Three Hours

3. Contact all operations, data preparation, admin staff, and 76 CommGp.
4. Inform all staff of the problem and the actions being taken.
5. Ensure all staff remain calm and understand their roles.
6. Inform all staff of any temporary instructions.

7. Inform all user contacts of the nature and extent of the problem. Telling them that they will be kept informed of the plans to recover.
8. Report back at the second meeting of recovery team leaders.

Within Twenty Four Hours

9. Contact suppliers of (If required):
 - Hardware.
 - Communications equipment.
 - Essential equipment.
10. Inform them of the arrangements for moving to the standby facilities.
11. Order new equipment and arrange to have it installed in the standby facility.
12. Initiate 'interim' back-up procedures for critical systems (this may involve manual procedures)
13. Brief all operations staff required to travel to the interim site(s).

Ongoing

14. Call all user contacts on a regular basis, advising them of the disruption and the actions being taken.
15. In conjunction with the Facilities Team, monitor the delivery and installation of any new/replacement hardware, communications and essential equipment.
16. In the light of the disruption, review all operational schedules in terms of jobs to be run, timings, priorities and dependencies.
17. Prepare schedules in readiness for start-up at the standby site.
18. Accept hand-over of standby site from the Facilities Team.
19. In conjunction with the Networks Team, initialise and test the systems:
 - hardware
 - operating systems
 - communications network
20. Before undertaking any processing, make backup copies of all files and programs.
21. Transfer security copies to off-site storage location.

4.3.3 Networks Team

Immediate

1. Alert and mobilize all other team members.
2. Attend the initial meeting called for recovery team leaders.

Within Three Hours

3. Contact relevant staff with a networks responsibility; inform them of the problem and the actions being taken. Contact 76 CommGp concerning ITSS assistance.
4. Ensure that all staff remain calm and understand their roles.
5. Inform network staff of any temporary instructions.
6. Help to compile an inventory of surviving communications equipment (voice/data) and what is to be acquired.
7. Ensure that all relevant documentation is at hand or retrieved from the off-site storage facility, for the reinstatement of the network.
8. Liaise with the Operations Team as to the status of communications equipment and assist with acquiring replacement equipment if required.
9. Provide further information to enable the Communications Team to keep users informed of current position if required.
10. Ensure that all documentation/information is available for the Operations and Facilities teams in order to connect the voice, local and wide area network to the standby facility.

11. Liaise with the Standby Facility and telecom service providers (this would normally be through 76 CommGp) to monitor progress of communications reinstatement.
12. Report back at the second meeting of recovery team leaders.

Within Twenty Four Hours

13. Define the priorities for restoring the network on a gradual basis in order to provide a minimum initial communications requirement for normal operations.
14. Liaise with suppliers of communications equipment to ensure prompt delivery, if required.
15. In conjunction with the Operations Team, ensure that the reinstated communications network is operable and tested.
16. Provide ongoing support for the communications network and carry out any re-configuration of the reinstated network that may be necessary.
17. Attend the third meeting of the disaster recovery team leaders and report the restoration status.

Ongoing

18. In conjunction with the Operations Team, monitor the network's performance.
19. Monitor and deal with users' requests in the light of the restricted network.
20. Prepare an inventory of all communications equipment requiring replacement in order for the original IS environment to be re-utilised.
19. Order replacement equipment as required in conjunction with the CIO and senior Materiel Group staff.

4.3.4 Accommodations Team

Immediate

1. Provide an initial damage report to *the Disaster Management Team Leader*.
2. Alert and mobilize all other team members.
3. Attend the initial meeting called for recovery team leaders.

Within Three Hours

4. Conduct an asset inventory.
5. Make a full evaluation of the damage.
6. In conjunction with the Operations Team identify all potentially salvageable equipment.
7. Carry out safety inspections.
8. Make the site secure, to prevent unauthorised access by staff or the public.
9. Estimate the time required to recover.
10. Report back at the second meeting of recovery team leaders.

Within Twenty Four Hours

11. Provide the required facilities at the Command Centre.
12. Arrange hotel or other temporary accommodation for staff if required.
13. Set up transport arrangements to/from all temporary locations.
14. Set up an Administration Support Desk to handle all queries.
15. Transfer staff to temporary locations.
16. Remove vital documents from disaster site.
17. Remove re-usable equipment from disaster site.

Ongoing

18. Set up administrative support services:
 - typing/word processing
 - telephones

- fax
 - mail - internal/external
 - office equipment
 - stationery
19. Remove salvaged items from the disaster area.
 20. Set up security procedures at the standby facility.
 21. Contact suppliers of essential services and make any arrangements required as a result of the disruption.
 22. Supervise delivery and installations at the standby facility.
 23. Monitor the installation of:
 - electricity
 - heating/lighting
 - air conditioning
 - fire detection systems
 - access control systems
 - telephones.
 if these need to be provided at the standby facility.
 20. Provide office furniture for the standby facility if required.

4.3.5 Communications Team

Immediate

Alert and mobilize all other team members.

Attend the initial meeting called for the recovery team leaders.

Set up the Crisis Desk to handle all communications (may be located in the Command Centre).

Within Three Hours

1. Liaise with the Management Disaster team to agree on the information to be communicated.
2. If applicable, make initial calls to suppliers of the following and inform them of the disruption and the likely demands to be made on their time and services:
 - standby facility
 - hardware
 - software
 - communications equipment
 - other equipment
 - utilities (electricity, gas, water)
3. If applicable, make calls to Materiel Group clients and inform them of any potential delays.
4. If applicable, issue a statement to local, national and international Press, as appropriate.

Within Twenty Four Hours

5. Advise all user departments of the transition plans and the arrangements during the period prior to the actual transition.

Ongoing

6. Handle all public relations issues.

4.4 Command Centre

This section describes the Command Centre, from where the Disaster Management Team will direct disaster recovery operations.

4.4.1 Primary Command Centre

If the Materiel Group premises at NDHQ are intact following the disaster, the command centre will be located at: 16th North Tower, Pearkes Building. Or any other location as determined by the ADM(Mat) in consultation with ADM(IM) and CFSU.

4.4.2 Alternative Command Centre

If an alternative command centre is necessary, the command centre will be located at: Louis St Laurent Building in Gatineau Que. Or any other location as determined by the ADM(Mat) in consultation with ADM(IM) and CFSU.

4.4.3 Command Centre Requirements

The command centre will be the focal point of all disaster recovery. The command centre shall be staffed by personnel, who have the resources, knowledge, and authority, to provide coordination for all DR initiatives; respond to inquiries from the user community; and requests for new direction by the recovery teams.

The following command centre resources may be required, and will be supplied by the team indicated.

Item:	To be supplied by team:
Business Continuity Plan	BCP Management Team
Whiteboard / flip chart & stand	Accommodations Team
Secure voice (STU III)	DMIS 3
Contact Lists	Divisional Support Staff
Telecom telephone directory	Accommodations Team
Desks, chairs	Accommodations Team
Telephone lines	Networks Team
Dedicated lines	Networks Team
Mobile phones	Networks Team
Fax machine	Accommodations Team
Photocopier	Accommodations Team
Classified waste disposal	Accommodations Team
Tool kit (cables and plugs)	Accommodations Team
Office supplies	Accommodations Team
Refreshments (coffee, tea and so on)	Accommodations Team
Camp beds	Accommodations Team
Shower facility	Accommodations Team
Car parking	Accommodations Team
First aid kit	Accommodations Team
Refrigerator	Accommodations Team
Microwave oven	Accommodations Team

4.5 The Standby Facility

This section provides a general introduction to the standby facility, which the Materiel Group can utilise for computer processing following a disaster.

It provides detailed information on preparing the facility. This information includes the following:

- Network (data and voice communications)
- Hardware configurations
- Security

4.5.1 Location of the Standby Facility

The address of the Standby Facility is: Louis St Laurent, 555 Boul De La Carriere, Gatineau Que. Or any other location as determined by the ADM(Mat).

5 Influenza Pandemic Response

5.1 In an Event of an Influenza Pandemic

(Currently waiting PMed Instructions on how to deal with an Influenza Pandemic, these instructions are for the short term)

Immediate

1. Provide Influenza Pandemic Kit to personnel with high exposure.
2. Restrict workplace entry of people with Influenza Symptoms.
3. Post notices at all entry Points.

Within Three Hours

4. Post hygiene notices at entrances, washrooms, hand washing stations, and public areas.
5. Assess each person that comes in the building.
6. Hand out Influenza Pandemic Kit at building entrances.
 - a. Includes:
 - i. Mask
 - ii. Gloves
 - iii. Hand sanitizer
 - iv. Brochure: Staying Healthy and Minimizing Influenza Transmission.
 - v. Document: Influenza Pandemic Policy.

Within Twenty Four Hours

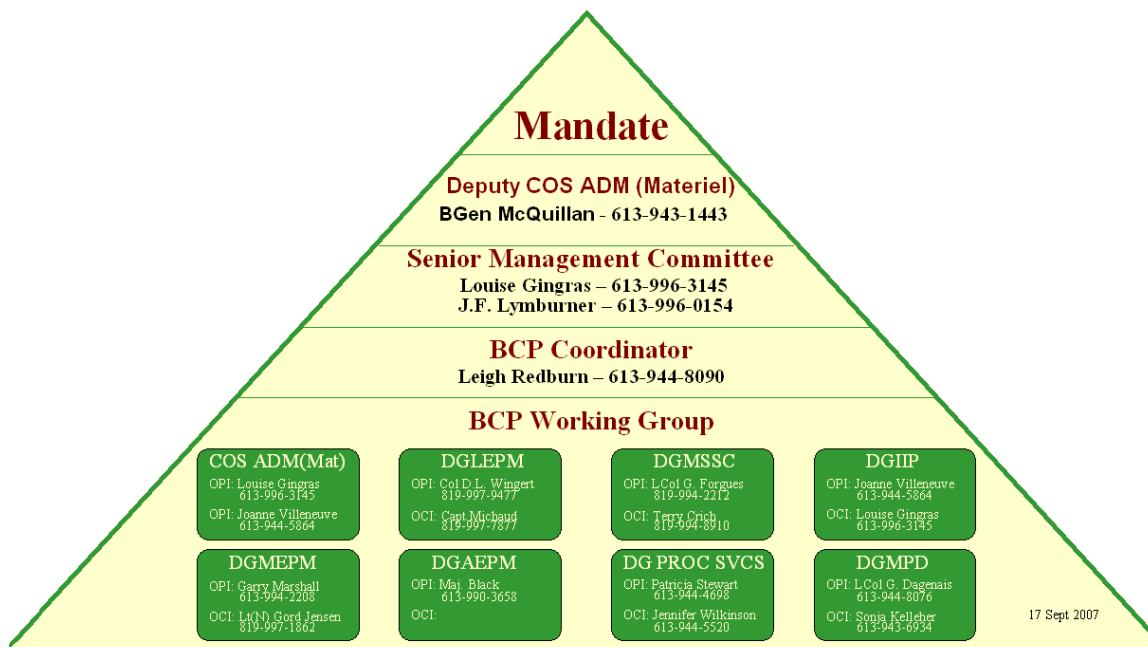
7. Maintain essential Business Operations define in BCP.
8. Cease non-essential Business Operations.

Ongoing

9. Hand out Influenza Pandemic Kit at building entrances.
 - a. Includes:
 - i. Mask
 - ii. Gloves
 - iii. Hand sanitizer
 - iv. Brochure: Staying Healthy and Minimizing Influenza Transmission.
 - v. Document: Influenza Pandemic Policy.

(Intentionally Blank)

ANNEX A
ADM(Mat) BCP Governance Structure



ADM (Mat) BCP Team Contacts

ADM(Mat) Executive BCP coordinator: Louise Gingras

ADM(Mat) Executive BCP coordinator: J.F. Lymburner

ADM(Mat) BCP Planner : Leigh Redburn

GROUP	DIVISION	DIRECTOR GENERAL	OPI	OCI
ADM(Mat)	COS ADM (Mat)	DEP. COS BGen McQuillan	Louise Gingras	Joanne Villeneuve
ADM(Mat)	DGLEPM	BGen J.C.M. Giguère	Col D.L. Wingert	Capt M Michaud
ADM(Mat)	DGMSSC	Larry M. Lashkevich	Lcol G. Fergues	Mr. Terry Crich
ADM(Mat)	DGIIIP	John Neri	Joanne Villeneuve	Louise Gingras
ADM(Mat)	DGMEPM	CMDRE R.W. Greenwood	Garry Marshall	Lt(N) Gord Jensen
ADM(Mat)	DGAEPM	BGen P.J. McCabe	Maj. Black	N/A
ADM(Mat)	DG PROC SVCS	Mariette Fyte-Fortin	Patricia Stewart	Jennifer Wilkinson
ADM(Mat)	DGMPD	Paul Labrosse	LCol G. Dagenais	Sonja Kelleher

CONTACT INFORMATION

Name	Rank	Phone	Cell Phone	Fax	Internal E-Mail	External E-Mail
Black, D	Major	613-990-3658	N/A	613-993-2764	Black Maj DR@ADM(Mat) DAEBM@Ottawa-Hull	Black.DR@forces.gc.ca
Crich, Terry	Civ	819-994-8910	613-868-7552	819-994-9398	Crich TJ@ADM(Mat) DQA@Ottawa-Hull	Crich.TJ@forces.gc.ca
Stewart, P	Civ	613-944-4698	N/A	613-995-1826	Stewart PA@ADM(Mat) DG Proc Svcs@Ottawa-Hull	Stewart.PA2@forces.gc.ca
Dagenais, G	LCol	613-944-8076	N/A	613-943-6977	Dagenais LCol JDG@ADM(Mat) DMPS@Ottawa-Hull	Dagenais.JDG@forces.gc.ca
Fergues, G	LCol	819-994-2212	N/A	819-997-3524	Fergues LCol JRG@ADM(Mat) D TN@Ottawa-Hull	Fergues.JRG@forces.gc.ca
Gingras, Louise	Civ	613-996-3145	N/A	613-995-2305	Gingras LG@ADM(Mat) DMGMC@Ottawa-Hull	Gingras.LMJ@forces.gc.ca
Kelleher, Sonja	Civ	613-943-6934	N/A	613-943-6877	Kelleher SL@ADM(Mat) DMPS@Ottawa-Hull	Kelleher.SL@forces.gc.ca
Marshall, G	Civ	613-994-2208	N/A	819-997-2194	Marshall GW@ADM(Mat) DMMS@Ottawa-Hull	Marshall.GW@forces.gc.ca
Jensen, Gord	Lt(N)	819-997-1862	N/A	819-997-2194	Jensen Lt(N) RG@ADM(Mat) DMMS@Ottawa-Hull	Jensen.RJ@forces.gc.ca
Neri, John	Civ	613-944-5864	613-818-2668	613-995-2305	Neri JP@ADM(Mat) DGIIIP@Ottawa-Hull	Neri.JP@forces.gc.ca
Michaud, C	Capt	819-997-7877	N/A	819-994-3143	Michaud Capt MMC@ADM(Mat) DLEPS@Ottawa-Hull	Michaud.MMC@forces.gc.ca
Smith, Patricia	Civ	819-997-5476	N/A	819-997-2883	Smith P@ADM(Mat) DMMS@Ottawa-Hull	Smith.PMC@forces.gc.ca
Villeneuve, Joanne	Civ	613-944-5864	613-818-2668	613-995-2305	Villeneuve J@ADM(Mat) COS ADM(Mat)@Ottawa-Hull	Villeneuve.JQ@forces.gc.ca
Wilkinson, Jennifer	Civ	613-944-5520	N/A	613-995-1826	Wilkinson JL@ADM(Mat) DG Proc Svcs@Ottawa-Hull	Wilkinson.JL@forces.gc.ca
Wingert, D.L	Col	819-997-9477	613-286-1104	819-994-3143	Wingert Col DL@ADM(Mat) DLEPS@Ottawa-Hull	Wingert.DL@forces.gc.ca

Last Updated: 17th Sept 2007
Last Verified: N/A

ANNEX D

Emergency Services

Service	Phone	Address
Military Police	613-995-0123	Pearkes Building
Local Police	613-230-6211	Ottawa City Police
Hospital (HCC)	613-945-6652 – Non-working hours, 613-945-6600 – working hours.	CFSU Ottawa HCC
Local Hospital	613-737-8000, 819-595-6000,	Emergency Services, General Campus; Hopital de Hull;
Ambulance	911	Throughout the NCR
Fire Departments	911	Through out the NCR
Gas Escapes (24 hours)	1-800-463-1850	PWGSC – Building Maintenance
Electricity	1-800-463-1850	PWGSC – Building Maintenance
MAN Help Desk	613-992-4000	Constitution Building
Water	1-800-463-1850	PWGSC – Building Maintenance
Burst Pipes (24 hour)	1-800-463-1850	PWGSC – Building Maintenance

ANNEX E

Other Contacts

Divisional ISSO:

DGLEPM, Omar Jaber 819-997-5142;
 CANOSCOM, Shewaye Gebremedhin 996-6173;
 DGMEPM, Lesley Wilson 819-994-8635;
 DGAEPM, Lisa Varin 613-998-8912;
 DGMSSC, Roger Rowley 819-997-3865;
 PMO MHP, Maj Andre Vanderpluym, 613-991-5004;
 PMO MASIS, Mr Sean Allen, 613-996-1924, and
 QETE, Mr Dave Belanger, 819-997-90769.

Divisional OPI:

DGLEPM, Capt St-Gelais, 819-997-9612;
 DGMEPM, Michel Brisebois, 819-994-8395;
 DGAEPM, Lcol Borys, 613-998-3774;
 CANOSCOM, Lcol Desrochers, 613-9924047;
 DG Proc Services, Lorraine de Puyjalon, 613-943-8204;
 COS ADM(Mat), Louise Gingras, 613-996-3145;
 DGMPD, Jason Choueiri, 613-943-5441;
 PMO MHP, Drew Mather, 613-998-6918;
 DGMSSC, Elwyn Tiegs, 819-994-8313.

Divisional CSM:

COS ADM(Mat), Lambert Broeren, 613-996-2731;
 DGLEPM/DG Proc Services, Nathalie Houle, 819-997-2676;
 CANOSCOM, George Koutakos 613-996-7535,
 DGMEPM, Dave Atkins, 819-994-5286;
 DGAEPM, Lisa Varin, 613-998-8912;
 DGMSSC, Heather Homuth, 819-994-1845;
 DGMPD, Karin Hendriksen, 613-944-8909.

ANNEX F

Plan Distribution List

Team	Recipient	Location	Electronic
------	-----------	----------	------------

			or Hardcopy
DND/CF BCP MG	LCol Jerry Walsh Cathy Cowan	Walsh LCol JF@SJS Plans@Ottawa-Hull 613-996-1438 Pearkes, 12CBS S011 Cowan CJ@ADM(Fin CS) DGCSS@Ottawa-Hull 613-944-6317 60 Queen St., 8 812	
DND Business Continuity Management Team	BGen McQuillan Louise Gingras Leigh Redburn	McQuillan BGen ME@ADM(Mat) COS ADM(Mat)@Ottawa-Hull Pearkes 16NT DD05 613-943-1443 Gingras L@ADM(Mat) DMGMC@Ottawa-Hull 613-996-3145 Pearkes, 10CBS S007 Redburn LR@ADM(Mat) DMGMC@Ottawa-Hull 613-944-8090 Pearkes, 10CBS L006	
ADM(IM) BCP Coordinator			
76 Comm. Group			
Accommodations Team			
Transportation Team			
CFSU (Ottawa) Operations Team			
IM/IT Security			

ANNEX G

76 COMM GP INCIDENT SERVICE RESPONSE TARGETS

1. Incidents are defined as any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.

2. Incident/Problem Management is the resolution and prevention of incidents that affect the normal running of an organisation's IT services. This includes ensuring that faults are corrected, preventing any recurrence of these faults, and the application of preventative maintenance to reduce the likelihood of these faults occurring in the first instance. The effective practice of both Incident and Problem Management will ensure that the availability of IT services is maximised, and may also protect the integrity and confidentiality of information by identifying the root cause of a problem.

3. All incidents, problems and service requests received by the ESP, either via a call to the Service Desk or through contact with other support groups, are opened as an incident tracking tool ticket. The status is maintained for each ticket to ensure it is tracked to completion and is handled in accordance with prescribed service levels.

4. Incidents have associated response and resolution time targets. The Service Desk will monitor all tickets opened. The Standard of Support for Incident Service Response is as follows:

Severity Level	Characteristics	Impact	Mean Time to Respond	Target Resolution Time
1	Total Service Outage at one or more sites	Infrastructure - Critical File/Print server down Network Failure Power Outage Virus detected on File/Print server	20 minutes	2 hours
2	Multiple Workstations at one or more sites	Workstation Priority Service Network connected workstation with virus Mission Critical workstation down; production deadline of today; no alternate workstation available Password reset for network workstation	20 minutes	4 hours
3	Service outage or severe performance degradation affecting many users at one or more sites	Infrastructure Performance Uncharacteristically slow network or server response Group of users on a server not functioning normally (i.e. Drive rights corrupt)	2 hours	4 hours
4	Major impact on as few as one user when no alternative workaround is available	Workstation (DWAN and Stand-alone) No access to "Standard" applications Workstation down preventing client from working (no alternate workstation available) Password reset for workstation not accessible to our network (i.e. Secure segments) "Standard" application not functioning (won't execute, producing errors, critical feature not working)	4 hours	24 hours
5	Incident affecting an individual user or a small number of users. Incident has a low impact level. Alternative workaround level is available.	User Problem Non-network connected workstation with virus Workstation down; alternative workstation available Shared printer down	24 hours	48 hours
6	Impact is limited in nature and not business critical	Other Local peripheral such as Printer, PDA, etc.) problem (down, noisy) Unsupported product (not functioning properly)	48 hours	96 hours

Severity Level	Characteristics	Impact	Mean Time to Respond	Target Resolution Time
		DND Home PC not functioning (May require return to DND hardware support)		