

IRM-5239-09

U.S. Marine Corps



CONTINGENCY PLANNING

PCN 189 523909 00

5239/09
CCIS-31
5 Jul 89

From: Commandant of the Marine Corps

Subj: CONTINGENCY PLANNING

Ref: (a) MCO P5510.14
(b) CMC Washington DC 270031Z Jul 88
(c) MCO 5271.1
(d) MCO P5600.31

Encl: (1) IRM-5239-09

1. PURPOSE. To provide guidance for preparing contingency plans as required by reference (a) and outlined for execution within reference (b). The objective is to ensure that personnel involved in the planning process are aware of the types of information which should be included in such plans and to provide a structure.

2. AUTHORITY. This publication is promulgated under the authority of reference (c).

3. APPLICABILITY. The guidance contained in this publication is applicable to all Marine Corps Central Design and Programming Activities (MCCDPA's), Regional Automated Services Centers (RASC's), Remote Job Entry (RJE) facilities, Deployable Force Automated Services Centers (DFASC's), and Department level and other small scale computers located in user work spaces. This guidance is applicable to the Marine Corps Reserve.

4. DISTRIBUTION. This technical publication will be distributed as indicated. Appropriate activities will receive updated individual activity Table of Allowances for Publications. Requests for changes in allowance should be submitted in accordance with reference (d).

5. SCOPE

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized only by CMC (CC) on a case by case basis.

6. RECOMMENDATIONS. As Marine Corps data processing activities gain experience in contingency planning, changes will be made to this technical publication to reflect actual experience. Recommendations concerning the contents of this technical publication should be forwarded to CMC (CCI) via the appropriate chain of command. All recommended changes will be reviewed upon receipt and implemented if appropriate.

7. SPONSOR. The sponsor of this technical publication is CMC (CCI).

R. L. PHILLIPS
Brigadier General, U. S. Marine Corps
Director, Command, Control, Communications and
Computer (C4) Division

UNITED STATES MARINE CORPS
Information Resources Management (IRM) Standards
and Guidelines Program

Contingency Planning
IRM-5239-09

Enclosure (1)

RECORD OF CHANGES

Log completed change action as indicated.

Change Number: _____

Date of Change: _____

Date Received: _____

Date Entered: _____

Signature of Person
Entering Changes

PUBLICATION TABLE OF CONTENTS

	Paragraph	Page
Chapter 1 GENERAL		
Section 1. INTRODUCTION	1.1.	1-3
Chapter 2 COMMAND RESPONSIBILITIES		
Section 1. ROLE OF MANAGEMENT	2.1.	2-3
Section 2. RISK MANAGEMENT	2.2.	2-3
Section 3. CRITICAL DEPENDENCIES	2.3.	2-4
Section 4. REVIEW AND APPROVAL	2.4.	2-5
Chapter 3 THE CONTINGENCY PLAN		
Section 1. PLAN DEVELOPMENT	3.1.	3-3
Section 2. PHASES	3.2.	3-3
Section 3. ALL PARTS EQUALLY IMPORTANT	3.3.	3-3
Section 4. PLAN FORMAT AND CONTENT	3.4.	3-5
Section 5. INTRODUCTION	3.5.	3-5
Section 6. PREPARATORY ACTIONS	3.6.	3-9
Section 7. ACTION PLAN	3.7.	3-15

Chapter 4
TESTING

Section 1. CONTINUAL EVALUATION	4.1.	4-3
Section 2. TEST PLANS	4.2.	4-3
Section 3. CONDUCTING TESTING	4.3.	4-3
Section 4. TEST PLAN DOCUMENTATION	4.4.	4-4

APPENDICES

A. GLOSSARY	A-1
B. REFERENCES	B-1
C. CONTINGENCY PLAN OUTLINE	C-1

Chapter Table of Contents

Chapter 1

GENERAL

	Paragraph	Page
Section 1. INTRODUCTION	1.1.	1-3
Reliance on Computers.....	1.1.1.	1-3
Contingency Plan	1.1.2.	1-3
Major vs. Small Problems	1.1.3.	1-3
Who Should Plan	1.1.4.	1-3
Elements of a Plan	1.1.5.	1-4
Make the Plan Fit	1.1.6.	1-4

Chapter 1

GENERAL

1.1. INTRODUCTION

1.1.1. Reliance on Computers. The continued growth in the reliance on computers to support day-to-day operations has increased the importance of plans to prevent loss of their availability. Only a few years ago it was reasonable to consider the recourse of manual operations when Automated Information Systems (AIS's) became unavailable. Today, there are but few situations in which it is even possible to revert to manual processes. Thus, contingency plans are necessary to minimize the turbulence caused by unexpected losses of data processing support.

1.1.2. Contingency Plan. Security measures are employed to prevent, or at least, to detect, accidental or intentional disclosure, modification or destruction of data, or loss of the means of processing data. A contingency plan, on the other hand, is designed to reduce to an acceptable level the consequences of any loss of computer resources or capability. The purpose of a contingency plan is to minimize the consequences of unexpected events, regardless of the magnitude.

1.1.3. Major vs. Small Problems. The probability of the occurrence of an undesirable event is generally inversely related to its magnitude. Usually, the greater the catastrophe, the lower the probability that it will happen. Data processing operations are disrupted with far higher frequency by small problems than by large ones. There is another relationship which is quite important to the quality of contingency plans. The size or scope of a catastrophe and of its effect on data processing operations are often not directly related. In the absence of a good plan, minor damage can cause major problems. Conversely, with a good plan, even major damage may not result in serious losses.

1.1.4. Who Should Plan. This document is addressed primarily to the Directors of the Marine Corps Central Design and Programming Activities (MCCDPA's), Regional Automated Services Centers (RASC's), Remote Job Entry (RJE) facilities, Deployable Force Automated Services Center (DFASC's), and Officers-in-Charge of Department level and other small scale computers in the user work space. (The term activity director will be used hereafter to denote responsible individual.) The guidance contained in this technical publication is also relevant to those organizations that are supported by the MCCDPA's, RASC's, RJE facilities, and to those organizations that operate computers in the user work space. This document may be used to establish requirements for adequate support during contingencies.

1.1.5. Elements of a Plan. The contingency plan will address the three elements described below.

a. Emergency Response. Procedures to cover the appropriate emergency response to a fire, flood, civil disorder, natural disaster, bomb threat, or any other incident or activity, to protect lives, limit damage, and minimize the impact on data processing operations.

b. Backup Operations. Procedures to ensure that essential data processing operational tasks can be conducted after disruption to the primary data processing facility. (Arrangements should be made for a backup capability, including the needed files, programs, paper stocks and preprinted forms, etc., to operate essential AIS's in the event of a total failure.)

c. Recovery Procedures. Procedures necessary to rapidly restore the data processing facility following physical destruction, major damage, or loss of data.

1.1.6. Make the Plan Fit. To the extent possible, the contingency plan should be clear and concise in order to facilitate its usefulness. The plan should be tested on a recurring basis and modified as changes in the data processing facility workload or equipment configuration dictate. Critical applications should be operated on the backup system at least annually to ensure that it can properly process this workload.

Chapter Table of Contents

Chapter 2

COMMAND RESPONSIBILITIES

	Paragraph	Page
Section 1. ROLE OF MANAGEMENT	2.1.	2-3
Duties	2.1.1.	2-3
Section 2. RISK MANAGEMENT	2.2.	2-3
Recognize the Consequences of a Disaster	2.2.1.	2-3
Risk Assessment	2.2.2.	2-4
Determine Acceptable Delay Time	2.2.3.	2-4
Section 3. CRITICAL DEPENDENCIES	2.3.	2-4
Resources	2.3.1.	2-4
Prioritize Requirements	2.3.2.	2-5
Section 4. REVIEW AND APPROVAL	2.4.	2-5
Objectives	2.4.1.	2-5

Chapter 2

COMMAND RESPONSIBILITIES

2.1. ROLE OF MANAGEMENT. Activity directors must recognize the importance of contingency planning. Contingency plans, if carefully prepared and executed, serve to keep within tolerable limits the consequences of losses or damage to computer resources. Economic feasibility in contingency plans requires carefully derived decisions as to what organizational functions are deferrable and for how long. Such decisions cannot be made without input from supported organizations. Activity directors are not in a position to assess the relative importance of work done within respective supported organizations. Further, the relative cost of continued support of each in the face of adversity may vary quite widely. Thus, cost of support under unusual conditions must be considered. For these reasons, it is essential that activity directors actively perform contingency planning in order to ensure essential support following disruption of services.

2.1.1. Duties. Activity directors should:

- a. Establish contingency plans which are based on the results of a comprehensive risk analysis.
- b. Conduct periodic tests of the workability of the contingency plan.
- c. Revise the plan as necessary. A complete review of the plan should be made upon the implementation of new AIS's, completion of a risk assessment, or a change in any of the critical dependencies.

2.2. RISK MANAGEMENT

2.2.1. Recognize the Consequences of a Disaster. The successful development of a contingency plan is dependent on recognizing potential consequences of undesirable events against which the facility needs protection. The facility is an assemblage of hardware, software, power, environmental controls, as well as the physical plant. However, all resources are not equally important. There is not equal susceptibility to harm (accidental or intentional), or to the consequences of such harm. Cost-effective protection of a data processing facility is heavily dependent on:

- a. An awareness of the facility's relative dependence on each of its component parts.
- b. Knowing the probability that an undesired event will happen to each component.
- c. A determination of the ramifications of undesired events in order to take appropriate actions to minimize either the chances of the event happening, the loss, or both.

2.2.2. Risk Assessment. Risk assessment is the process which provides the basis for selecting cost-effective security measures. The maximum allowable cost of any safeguard is limited by the size of the expected losses which will be mitigated by that safeguard. Any safeguard or combination of safeguards must not cost more than tolerating the problems to which the safeguards are addressed. Knowledge of the consequences of not being able to perform each system function for specific time intervals is essential to the creation of a contingency plan which is adequately responsive to the needs of the supported organizations.

2.2.3. Determine Acceptable Delay Time. A portion of the work-load may be deferrable for long periods before the deferral significantly impacts mission performance. Conversely, portions of the workload cannot be disrupted. The risk assessment must identify tolerable time delays.

2.3. CRITICAL DEPENDENCIES

2.3.1. Resources. The prompt recovery of a data processing activity from a loss of capability is dependent upon the availability of a variety of resources. The specific resources required are a function of the nature of the problem which generated the need for recovery. Some of these resources are absolutely essential to operations and, as such, are critical dependencies which warrant special care to ensure continuing availability and early recognition of a loss of capability.

a. Identify Critical Data. Special care must be placed on identifying data needed for backup and recovery purposes. There is often a certain amount of data which is absolutely vital to an organization, and which would have the first priority in any emergency situation. This data must be identified to facilitate its availability. Much of the remaining data is extremely useful to an organization and could be very costly to recreate. This type of data should also be properly categorized and maintained. Activity directors must ensure that backup copies are routinely prepared and maintained to provide acceptable service during backup and recovery situations.

b. Exercise the Contingency Plan. Activity directors must take steps to ensure the continuing availability of organic resources. More difficult, but no less important, is the firm commitment to the contingency plan of non-organic resources. The external commitments of critical resources must be reviewed frequently to see that they have not been forgotten or otherwise neglected by the organizations making those commitments. Periodic testing is the most satisfactory way of assuring the adequacy of such commitments.

2.3.2. Prioritize Requirements. After disruption to processing, it is seldom operationally or economically feasible to continue all processing support at an alternate location. The tasks performed by the activity are not all of equal importance. Further, the relative importance of an AIS may vary with time of day and day of week or month. A plan which attempts to provide the means to continue all processing without regard to relative importance will require costly backup capabilities which must be frequently exercised to assure availability and compatibility with normal activities.

2.4. REVIEW AND APPROVAL. The review and approval process for a contingency plan should be carefully established.

2.4.1. Objectives

a. Make commanders aware of any dependencies upon them for supportive action. Ensure that commanders realize that during an emergency, there may be some services which will not be provided, and will be otherwise unavailable.

b. Obtain command agreement on the assumptions on which the plan is based, including the dependence on other organizations for assistance.

c. Communicate to all supported commands the existence of a plan and obtain approval of the plan.

d. Obtain formal concurrence of any organizations upon which there might be dependence.

e. Inform and receive acknowledgment from all key personnel of their respective roles in the various recovery scenarios.

Chapter Table of Contents

Chapter 3

THE CONTINGENCY PLAN

	Paragraph	Page
Section 1. PLAN DEVELOPMENT	3.1.	3-3
Section 2. PHASES	3.2.	3-3
Preparation Phase	3.2.1.	3-3
Action Phase	3.2.2.	3-3
Section 3. ALL PARTS EQUALLY IMPORTANT.....	3.3.	3-3
Preliminary Planning	3.3.1.	3-3
Preparatory Actions	3.3.2.	3-3
Actions Plan	3.3.3.	3-4
Section 4. PLAN FORMAT AND CONTENT	3.4.	3-5
Section 5. INTRODUCTION	3.5.	3-5
Purpose	3.5.1.	3-5
Scope	3.5.2.	3-5
Assumption	3.5.3.	3-5
Responsibilities	3.5.4.	3-6
Strategy	3.5.5.	3-6
Change Log	3.5.6.	3-7
Security of the Plan	3.5.7.	3-8
Section 6. PREPARATORY ACTIONS	3.6.	3-8
Personnel	3.6.1	3-8
Data	3.6.2.	3-9
Application Software	3.6.3.	3-10
Computer Equipment and System Software	3.6.4.	3-10
Data Communications	3.6.5.	3-10

Supplies	3.6.6.	3-11
Transportation	3.6.7.	3-12
Facilities	3.6.8.	3-12
Power and Environmental Controls	3.6.9.	3-13
Documentation	3.6.10.	3-14
Section 7. ACTION PLAN	3.7.	3-14
Emergency Response	3.7.1.	3-14
Backup Operations	3.7.2.	3-14
Recovery Actions	3.7.3.	3-15

Chapter 3

THE CONTINGENCY PLAN

3.1. PLAN DEVELOPMENT. A systematic approach to developing and documenting the contingency plan must be followed to ensure successful implementation. Activity directors must ensure that all important areas are addressed and that the plan is structured to permit ease of reference to sections of significant interest or concern.

3.2. PHASES. A contingency plan shall consist of three parts which address two distinct, mutually exclusive sets of activity.

3.2.1. Preparation Phase

a. Part One, Preliminary Planning

b. Part Two, Preparatory Actions

Note: (These two parts should cover those things which should be or have been done in anticipation of a loss to lessen the damage or assist recovery.)

3.2.2. Action Phase

a. Part Three, Action Plan

Note: (This part should cover those things which must be done after the fact to minimize the cost and disruption to the supported organizational functions.)

3.3. ALL PARTS EQUALLY IMPORTANT. Each part of the plan is essential to its overall workability and effectiveness; therefore, no part should be considered more important than another. There are differences, however, in the manner of their presentation.

3.3.1. Preliminary Planning. Part One, Preliminary Planning, which is the basic driver of actions to take in the succeeding parts, should be completed prior to beginning the actual preparation of the remaining parts of the plan.

3.3.2. Preparatory Actions. Part Two, Preparatory Actions, describes specific preparation steps in a number of areas relevant to the facility and should be developed in as much detail as seems potentially beneficial. Such material should consist of "how to" instructions, and lists of information to the extent necessary. There will be time to read this material, to become educated in the problems and their potential solutions, to weigh alternatives and to select appropriate measures. An essential element of this part of the plan is unwavering insistence that all personnel on whom there is significant dependence during contingency operations be familiar with their potential respective roles, i.e., when implementing Part Three of the plan. These individuals are selected because they already know "how to". The plan must not be based on the assumption that the document describing it can be retrieved after the catastrophe by those with a role in recovery who will then read the plan to learn how to do what is needed of them. Except for supporting data from Part Two (such as personnel rosters listing telephone numbers, addresses, and job skills), it should not be necessary to read the plan to initiate contingency operations.

3.3.3. Action Plan. Part Three, Action Plan, should consist of clearly stated actions which are to be taken upon the occurrence of an emergency. Part Three is divided into three sections: Emergency Response, Backup Operations, and Recovery Actions. Each of the three sections includes those things which are to be done in response to a set of problem scenarios. These problem scenarios are derived in a large part from information in the risk assessment process and from practical working experience. They must be representative of the reasonable anticipated problems. Immediately following each problem statement or scenario should be a description of what is to be done in each category described (not how). One scenario may require actions, and be listed, in one or more sections of this part, e.g., a bomb threat (which does not result in any damage), minor power outages, etc., may necessitate action only under Section One, Emergency Response. A sustained power outage would involve action under Section One and Section Two, Backup Operations. An incident causing serious damage to the facility would, most likely, require steps under Sections One, Two, and Three, Recovery Actions. Examples of typical scenarios and sections of the plan which might apply include:

- a. Section One. A bomb threat which does not result in any actual damages, or a minor power outage.
- b. Sections One and Two. Fire or structural damage elsewhere in the building resulting in no loss of life has resulted in denial of access to the data processing facility for three days. Return to the facility after that period is anticipated, but it might be slightly longer.
- c. Sections Two and Three. Destruction of the facility with loss of all personnel working at this time.
- d. Sections One, Two, and Three. Total communications failure.
- e. Sections One, Two, and Three. A hurricane, earthquake, tornado, or other natural disaster occurs which cripples local transport, power and communications but does little physical damage to the facility.

(The scenarios mentioned above are not necessarily appropriate to any particular facility. The ones which are must be selected and be sufficiently large in number and breadth that they offer useful guidance in directing recovery in actual loss situations and in the performance of tests and rehearsals.)

3.4. PLAN FORMAT AND CONTENT. The content of the contingency plan is described in the following sections. A sample contingency plan format is contained in Appendix C.

3.5. INTRODUCTION. This part of the plan should describe the purpose, scope, assumptions, responsibilities, and overall strategy relative to the plan. Misconceptions concerning these concepts are

quite common and must be clearly addressed to ensure that they are communicated to those who must effectively respond to a contingency by implementing the plan. This part should conclude with a section which provides for recording changes to the plan. Each section of Part One and recommended contents are described below.

3.5.1. Purpose. This section should describe the purpose of the contingency plan.

3.5.2. Scope. This section should describe in concise terms the extent of the plan's coverage. For example, "This plan is applicable to the RASC, Camp Pendleton and all supported RJE facilities." Subordinate plans should also be provided in this paragraph.

3.5.3. Assumptions. A contingency plan is based on the assumptions derived from the risk assessment. The following guidance is provided to identify the plan's assumptions.

a. Nature of the Problem

(1) The general nature and range of events against which the plan is directed.

(2) Events not addressed by the plan which, because of their low probability, do not warrant consideration in the plan.

(3) Events which are so extensive in scope as to negate the feasibility for early recovery of data processing operations.

(4) Events too minor in scope to warrant reflection in the plan. These are generally sufficiently frequent as to be considered a normal part of the operation and which are now accommodated routinely.

b. Priorities. The assumptions must reflect how the priorities were determined. The data sources, the extent of user agreement on the selected priorities, the risk assessment methodology, and other related matters should be described in detail so as to convey a full understanding of the relative priorities to be observed in recovery of operations and of the rationale used to establish those priorities. The relative criticality of the supported functions will vary with time of day, day of week, and of month. Where appropriate, the description of priorities should reflect that situation.

c. Support Assumptions. Recovery from any type of problem (except minor, and relatively frequent, problems) usually requires support from other data processing facilities. Assumptions relative to resources should include the following:

(1) Use of another data processing facility and its formal commitment of support.

(2) Availability of replacement hardware and licensed software.

(3) Availability of supplies possibly influenced by transportation problems in the event of a major problem.

(4) Availability of personnel. (The mobility of personnel (civilian and military) after a natural disaster is frequently overestimated, particularly when that mobility requires leaving dependents in less than desirable circumstances.)

(5) Responsiveness of public utilities, particularly if there is a natural disaster.

3.5.4. Responsibilities. This section assigns responsibilities for actions associated with preparing and executing the plan. It is critical that the plan clearly delineate the responsibility of each organization. Responsibilities should be assigned by billet, (e.g., shift supervisor, senior operator).

3.5.5. Strategy. The selection of appropriate strategies is based on the risk assessment and available support resources. Strategies for implementing the Emergency Response, Backup Operations, and Recovery Actions will be described in this paragraph. Information for use in developing strategies is categorized by area as follows:

a. Emergency Operations. The strategy for this section is to protect lives and property to the maximum extent possible.

When developing a strategy to cover specific events, more complex actions and planning are necessary and must cover a very wide range of potential situations. To illustrate, the strategy for coping with a severe hurricane is different from that for a minor, easily controllable fire which creates smoke in the data facility. In the first scenario, the strategy might include actions such as close the facility, secure/transfer critical files, and release all personnel to allow them to assist their families. In the latter example, the strategy could be simply to execute power down procedures and evacuate all personnel to a nearby assembly point. The strategies selected must provide a sufficient base upon which procedures can be devised which afford all personnel the immediate capability to effectively respond to emergency situations where life and property have been, or may be, threatened or harmed.

b. Backup Operations

(1) Reference (b) identified an interim and long term backup strategy. The RASC at Camp Lejeune was designated as the primary interim contingency backup site. The RASC at Camp Pendleton was designated as a secondary interim site in the event Camp Lejeune could not provide support. Long term plans are to use a newly constructed facility at Quantico, Virginia, scheduled for completion in FY93.

(2) The designated Marine Corps contingency backup facilities do not have sufficient equipment, personnel, or supplies to sustain the complete operational requirements of another Marine Corps facility. If a facility's workload is so large that there is no other facility available to process the workload, it may be necessary to divide the workload among two or more physical locations selected to offer reasonable probability that enough capability will be available to process the critical workloads. Contingency plans must not be limited to backup processing support provided by another facility. Resources or capabilities such as personnel, supplies, space, transportation, and remote site storage of backup files must be reflected in the overall contingency plan. Strategies for backup of resources must be mutually supportive of and compatible with overall contingency strategies. Strategies for operation when less than total operability is the problem must also be developed. One single strategy, as in the case of loss of a facility, is rarely adequate because of the need to respond a wide variety of problem scenarios.

c. Recovery Actions. The strategy for recovery must be linked closely with that of backup operations. Initiation of recovery actions may overlap, or be the next step after backup operations in restoring data processing capability after partial or complete destruction of the facility, or other resources. The wide variety and scope of actions involved in recovery may dictate separating the specific recovery actions into two categories, i.e., short term and long term. Strategies should be developed for the scenario that the facility is damaged and backup facilities are available for critical processing. This situation is heavily dependent on such factors as how long non-critical workload can be deferred and the continuing availability of equipment at the backup facility. The short term strategy might be to defer non-critical work until the facility is restored, or, if possible accomplish manual processing. The long term strategy could be to restore operations at the existing facility by using previously identified contractors and vendors for construction and other services needed.

3.5.6. Change Log. The change log will summarize changes to the contingency plan. It will include a brief description of the change to include:

- a. Date. The date the change/update is effective.
- b. Type of Change. Note that the entry is a deletion, modification, or an addition.
- c. Section(s) Affected. Identify section or sections of the plan which will reflect the change.
- d. Description of the Change. Brief description of the change and how it affects the plan.
- e. Reference. A reference or source of the change.

3.5.7. Security of the Plan. Once documented, the plan provides a significant amount of sensitive information about the organization which, if misused, could result in considerable damage. The plan will be marked For Official Use Only (FOUO) and be appropriately safeguarded to prevent dissemination to unauthorized personnel.

3.6. PREPARATORY ACTIONS. This section of the contingency plan will be a key part of the document to which reference is required to reestablish the data processing operation. It is very important that all personnel know their respective roles in recovery. This part of the plan is critical to the emergency response, backup and recovery from all but the most routine problems. This part is also the most frequently changed section of the document because it contains the lists of detailed information and procedures which are subject to frequent changes. Marine Corps data processing facilities support a wide variety of functional areas and organizations, require off-site record storage, and are dependent on telecommunications. Because of these factors, the preparatory actions must be clearly defined to ensure adequate backup and recovery of essential operations. The sections which should be considered for inclusion in the contingency plan are shown below, along with definitive information about the contents of each of the sections.

3.6.1. Personnel

a. Properly trained and motivated personnel are the most critical element to the graceful recovery from damaging losses. This is the most difficult element to factor realistically into a contingency plan. Because of this, workable plans are those that reflect this dependence on personnel and which accommodate the problems they present. Personnel can be expected to innovate, perform unfamiliar tasks, work under considerable stress and work long hours if they are in a reasonably familiar environment, particularly if they are not too deprived of the creature comforts found in their normal work environments. Personnel tend not to perform complex tasks well in a physical stressful environment unless there are also strong motivations for doing so.

b. When extreme weather conditions (floods, tornadoes, hurricanes) have created the need to invoke a contingency plan, personnel with dependents and material possessions (houses, cars, boats) are often reluctant to leave them exposed and not cared for to go to a geographically remote alternate site to effect backup operations or recovery of data processing operation. It is under stressful conditions that they often find a variety of reasons for not going, or that they do not effectively perform due to unhappiness or concern for that which they left behind. This situation must be considered when developing procedures for backup site operation. Without the necessary personnel, recovery will be virtually impossible.

c. It is assumed that the contingency plan will be formed about several problem scenarios ranging from disruptions caused by loss of local power (even with backup) or telecommunications, fire elsewhere in the building resulting in denial of access to the ADP facility, to major equipment failures, to intentional damage by malcontents, or to destruction of the facility by whatever cause.

d. This section will contain names, addresses, and telephone numbers of all personnel who will be required in any backup or recovery scenario. Prior compilation of this information is essential, as it cannot be assumed that upon occurrence of an emergency available personnel will be sufficiently knowledgeable

for a particular recovery situation. (See Sec. 3.5.4., Responsibilities.) Thus, it will be necessary on any list to associate personnel, skills, and billets in recovery. Alternates for personnel with skills in very short supply must be designated. Alternates should be selected from personnel not working the same shift or in the same physical area.

e. Key personnel required to support mission critical systems must be aware of the dependence of the plan on them. These personnel must be informed of their recovery responsibilities and roles, and the roles should be routinely rehearsed. Training must be provided to ensure that the necessary skills to effect recovery are available when needed.

3.6.2. Data

a. Data is subject to a variety of vulnerabilities. Data essential to backup and recovery must be adequately recorded, maintained in current condition, and backup copies adequately protected.

b. Metadata is contained in the activity's data dictionary. All metadata must be safeguarded in the same manner as data. Metadata is any data needed to define, file, or manipulate data, and/or data about interfaces between automated information systems (AIS's).

3.6.3. Application Software. Activity directors must ensure that mission critical AIS's are identified. Since application software is subject to change, care must be taken to ensure that current versions and supporting documentation are adequately safeguarded and readily available to meet contingency operations.

3.6.4. Computer Equipment and System Software. As required by reference (b), activity directors will review resources designated by RASC Camp Lejeune as available for use during periods of contingency. With respect to the available resources, activity directors will identify computer equipment and system software requirements that are not satisfied by the available contingency resources. It is critical that the designated backup facility and the potential users keep all computer equipment and system software inventories current. CMC (CCI) will initiate actions to reduce computer equipment and system software shortfalls and replace damaged equipment and/or software.

3.6.5. Data Communications. Data communications support is primarily provided by the Marine Corps Data Network (MCDN). The MCDN is a common-user data communications network which provides terminal-to-computer and computer-to-computer communications to Supporting Establishment (SE) and FMF units in garrison. Where possible, connectivity to MCDN will be extended to FMF units who are deployed. The MCDN architecture is based on the use of communications or front-end processors (FEPs) as the major nodal elements in the network. FEPs perform front-end processing for all host computers, switching/line control for all terminals, and other network communications functions. Connectivity between nodal points on MCDN is provided by a mixture of both leased and Defense Communications System (DCS) provided circuitry.

Connectivity for individual users, both individual terminals and network subscribers connected via Local Area Networks (LANs), is provided through either local (channel connection for users located nearest host computers, individual dedicated telephone lines supported by base cable systems, etc.) or remote multipoint connection to the nearest nodal point. Reconstitution of MCDN connectivity is supported in the following fashion.

a. Restoration of Service Between Primary MCDN Nodes. Currently, each Marine Corps Central Design and Programming Activity and Regional Automated Services Center has multiple communication paths (each node is connected to more than one MCDN node, either by single or multiple dedicated communication circuits). Both the primary and secondary communication circuit(s) between major nodes have been assigned restoration priorities in accordance with DCS management procedures which will cause the circuits to be restored should service be interrupted. As an alternative to restoration of dedicated

communications circuits between sites and in order to provide immediate restoration of service in the event of a major disruption of communications service MCDN nodes should plan for restoring trunk connectivity via dial-up access. Both the planning for and implementation of dial-up access as a means of restoring trunk circuit connectivity between MCDN nodes will be coordinated and controlled by CMC (CC).

b. Restoration of Service Between Secondary MCDN Nodes and Their Servicing Primary Nodes.

Currently, each MCDN Remote Job Entry (RJE) site is dual accessed (connected to a primary MCDN node by more than one dedicated communications circuit) to either a MCDN or RASC. Eventually, service to several MCDN subnodes (MCDN San Diego, MCDN El Toro, MCDN Harris Island and MCDN Cherry Point) will be reduced to a single 56KBPS digital link. In the event the communication link(s) between a secondary node and its servicing primary node are disrupted, service will be restored either through re-engineering of the circuit(s) based on DCS assigned restoration priority or via CMC (CC) authorized dial-up procedures. Each MCDN subnode should also plan for the manual delivery of data to their servicing primary node in the event of long term disruption of communications.

c. Restoration of Service to Locally Attached and Remote Network Subscribers. The responsibility to plan for individual site reconstitution rests with the activity director. Plans which call for the reconnection or restoration of MCDN access for channel attached or locally attached users, (e.g., Network users on or aboard a Marine Corps SE site) is the responsibility of the specific activity director. Restoration of service to subscribers at remote locations (such as I&I Staff/Reserve locations, Recruiting Stations, and Marine Corps Administrative Detachments, etc.) rests with the CMC (CC). In the majority of cases, service to remote users will be restored via dial-up to a major MCDN node. However, both locally attached and remote MCDN subscribers must plan for the manual transfer of data to a servicing MCDN or RASC in the event of a major disruption to communications.

3.6.6. Supplies

a. With exception of a very few items which might be peculiar to a particular facility, most supplies are catalog items with reasonable availability. However, for most facilities there is a sufficiently large number and variety of such items as to make plans for stockpiling a modest quantity at another, safe location a necessary step. When every effort is being made to restore operations, valuable time can be lost in locating things of limited dollar value, such as tape cleaners, floor tile pullers, labels, and marking pens. This time can be saved by advance planning for the availability of such items. The contingency planner should bear in mind that the provision of supplies is an important task that is a necessary part of recovery from a major disruption.

b. Particular care must be given to the continued availability of special forms on which there may be a critical dependence. The replacement lead time on these is often measured in weeks. An adequate buffer supply should be stored off-site in a location not generally susceptible to the problems reasonably anticipated at the normal storage location. This buffer supply should be sufficient in quantity to provide for 30 days usage or sufficient in quantity to cover the time period required for supply of those items that take longer than 30 days.

c. The Directors of RASC Camp Lejeune and RASC Camp Pendleton will review the requirements for special forms and miscellaneous supplies with the activities who will use the contingency site and ensure that an adequate inventory of supplies is on hand to satisfy contingency requirements.

3.6.7. Transportation

a. Events which disrupt transportation of personnel or supplies might have serious disruptive effects on the ability of data processing facilities to operate effectively. Of greater importance here, however, is the effect of loss of transport on recovery.

b. Area-wide power failures almost uniformly cripple all urban transport, including automobiles. Earthquakes make roads impassable. Labor difficulties can seriously impede public transport.

c. Activity directors will ensure that site contingency plans provide for the movement of personnel and required/ available material to the backup site. Liaison with local transportation personnel will aid in the planning for rapid displacement of personnel and material should the need arise.

3.6.8. Facilities

a. The provision of space into which a data processing facility can be placed after loss of an original site can be considered for two purposes, as follows:

(1) Space which can be used temporarily while the original site is being rehabilitated.

(2) Space into which the data processing operation can relocate with relative permanence.

b. Equally important as space for the data processing equipment are the arrangements that are required for the personnel who arrive from the affected site. Activity directors for the designated backup sites must work closely with all activity directors in determining such requirements as work space, billeting, and messing during periods of contingency. Options such as remote activities by programmers and analysts should be thoroughly reviewed.

3.6.9. Power and Environmental Controls

a. Uninterruptible Power Supply (UPS) systems provide three potentially useful functions. They are:

(1) Protection against power line transients which can provoke a system interruption requiring a restart and with the potential for damage to data.

(2) Provide a short period, usually from 15 to 30 minutes, in which the system can be stopped gracefully following a loss of primary power from a public utility.

(3) Provide a short period following a primary power failure, during which time a standby generator can be brought into operation to support the data processing operation or at least the critical functions.

b. The proper installation and maintenance of power and environmental equipment is as critical as that of the data processing equipment. Opportunities to learn valuable lessons in these areas have presented themselves in the past. Review of after action reports have provided the following:

(1) When designing an emergency power system, electrical power for the work spaces of key data processing personnel and key personnel of any other tenants of the building/site must be considered.

(2) Ensure vendor training is attended by a sufficient number of personnel to ensure that someone is always available with in-depth knowledge of the UPS. Also ensure that Base Maintenance personnel are knowledgeable about the functioning of UPS.

(3) Ensure proper preventative maintenance (PM) is performed in accordance with manufacturer's specifications. Remember proper cleaning of the equipment and its surroundings is a crucial part of the PM cycle.

(4) During upgrade of existing equipment/facilities or as acquisition of new equipment/facilities is being planned, equipment compatibility and reliability engineering must be considered. A regular, rigorous testing program that simulates an emergency and tests overall system performance under a full load is the

best way to know that each piece of equipment will operate satisfactorily in an emergency. Such a program will often reveal engineering errors and equipment incompatibility.

(5) In the event of partial failure of environmental controls, it may be possible to selectively power-down less needed equipment in order to keep the computer operational. To prepare for this eventuality, a list of equipment which might be temporarily taken out of service should be prepared and maintained.

3.6.10. Documentation. This section of the plan should describe all backup documentation which is kept in the off-site facility so as to facilitate its retrieval. Without clear, concise and complete documentation, all but the simplest operations could become very difficult to execute. A complete set of all pertinent documentation such as Computer Operation and User Manuals, should be stored in a secure off-site facility. Copies of the contingency plan and supporting documentation should likewise be stored in a secure location.

3.7. ACTION PLAN. This part of the plan should consist of the "what to" actions to be accomplished by those personnel or activities identified in section 3.5.4. Responsibilities. This part of the plan will consist of concise instructions describing specific actions to take as a response to each of the problem scenarios which were developed earlier for each of the three categories listed below.

3.7.1 Emergency Response. Include in this section the immediate actions to be taken in order to protect life and property and to minimize the impact of the emergency. It is recommended that a separate list of actions be developed and maintained for each of the problem scenarios such as bomb threats, power outages, air conditioning failure, or fire alarm. To facilitate use of the list of actions, more than one copy of each will be required in addition to the master, or file copy. The number required is dependent on the size of the facility and the ease with which needed sections may be retrieved for use. In any event, it should never be necessary to search for a needed portion of the plan after an emergency requiring its use has occurred. Following is an abbreviated example of the actions which might be included as a response to a sudden power outage of unknown duration (assuming UPS is installed and operative):

- a. Initiate power down procedures.
- b. Notify key personnel.
- c. Notify customers of disruption of service.

Note: The detailed instructions on how to accomplish the tasks listed above, and others as applicable to the facility should be located in "Preparatory Action" part of the plan under the specific categories.

3.7.2. Backup Operations. In this section, describe what must be done to initiate and effect backup operations, separately for each of the scenarios developed. For example, if the scenario is: major power outage of expected 3-day duration; backup operations at primary alternate facility necessary, the list of actions to take might include, but not be limited to:

- a. Notify alternate facility.
- b. Notify backup team.
- c. Notify customers of disruption of service.
- d. Arrange transportation.
- e. Retrieve backup supplies.
- f. Assemble copies of software, data, and documentation.

Note: Any "how to" instructions for each of the above areas should have been included in "Preparatory Actions" part of the plan.

3.7.3. Recovery Actions. As in the two preceding sections, the instructions in this section should be limited to describing what to do in effecting recovery from the situations documented in the problem scenarios. For example, if the scenario is: the data processing facility has been damaged, some equipment destroyed, but critical applications may continue to be processed. The action list in this case might reflect items such as:

- a. Perform survey to determine specific facility, hardware or data damaged and losses.
- b. Retrieve backup files, as necessary. (Consider the possibility that if the primary file is destroyed and if the only backup copy of the file is retrieved from the off-site storage, no further backup is available until the backup file is copied.)
- c. Report equipment requirements to CMC (CCI).

Chapter Table of Contents

Chapter 4

TESTING

	Paragraph	Page
Section 1. CONTINUAL EVALUATION	4-1.	4-3
Section 2. TEST PLANS	4.2.	4-3
Realistic Testing	4.2.1.	4-3
Mission Critical AIS Testing	4.2.2.	4-3
Section 3. CONDUCTING TESTING	4.3.	4-3
Section 4. TEST PLAN DOCUMENTATION	4.4.	4-3

CHAPTER 4

TESTING

4.1. CONTINUAL EVALUATION. One of the more important aspects of successful contingency planning is the continual testing and evaluation of the plan itself. Quite simply, a plan which has not been tested cannot be assumed to work. Likewise, a plan documented, tested once and then filed away to await the day of need provides no more than a false sense of security. Data processing operations are, historically, volatile in nature, resulting in frequent changes to equipment, programs, documentation, customer requirements, and often even in the way daily business is conducted. Because of this, the contingency plan must be considered a living document. The contingency plan must be subjected to continual management review and testing on a periodic basis. The contingency plan should be exercised at least annually.

4.2. TEST PLANS

4.2.1. Realistic Testing. The devising of test plans which adequately and reliably exercise the contingency plan themselves require considerable skill and great care so as meet the objective of providing tests which are entirely realistic while still being economically feasible.

4.2.2. Mission Critical AIS Testing. Care must be taken to see the tests involve the most important AIS's to be supported in the contingency environment. The testing of the simpler jobs may be desirable initially, but such tests do not provide adequate assurance that mission critical AIS's can be supported. Mission critical AISs are identified in the Mid-Range Information Systems Plan (MRISP) which is published annually.

4.3. CONDUCTING TESTING. It is generally only necessary to assume that operations at the home site are disrupted or otherwise not available. For example, it is not essential to have an actual fire in order to test the emergency evacuation procedures. What is needed is an understanding with the fire department and documentation of the specific test procedures to follow in simulating the fire and emergency condition. Likewise, to test backup operations at an alternate site, it is not mandatory to cease operations at the home site, but rather to gather copies of all needed data and other information required to actually begin operations at the alternate facility. In situations such as this, the test most heavily inconveniences the supporting (alternate) facility which is assumed to be unharmed in the simulated catastrophe or disruption of service.

4.4. TEST PLAN DOCUMENTATION. The test plans should form a formal part of the contingency plan documentation and be as fully subject to the review and approval process as the other sections of the plan.

APPENDIX A

GLOSSARY

Backup Operation: A method of operations to complete essential tasks (identified by the risk analysis) subsequent to disruption of the ADP facility and continuing until the facility is sufficiently restored.

Emergency Response: A response to emergencies such as fire, flood, civil commotion, natural disasters, bomb threats, etc., in order to protect lives, limit the damage to property and minimize the impact on ADP operations.

Mission Critical AIS: An AIS is considered mission critical when the information obtained from that AIS provides information critical to the accomplishment of a wartime mission and this information cannot reasonably be obtained through other means.

Recovery: The restoration of the ADP facility or other related assets following physical destruction or major damage.

Risk Assessment: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

APPENDIX B

REFERENCES

1. Federal Information Processing Guidelines for ADP
Standards Publication 87 Contingency Planning
2. National Bureau of Standards Guide on Selecting ADP
Special Publication 500-134 Backup Processing
Security Program
3. OPNAVINST 5239.1A Department of the Navy
Automatic Data
Processing Security Program
4. MCO P5510.14 Marine Corps Automatic Data Processing (ADP) Security Manual

APPENDIX C

CONTINGENCY PLAN FORMAT

NOTE: The exclusion of any item in the examples below does not imply that further entries may not be required for any facility. The purpose of the example entries is to suggest possible planners will undoubtedly discover that in order to provide complete coverage, further expansion of the outline will be necessary.

Part One-Preliminary Planning

1.1 Record of Changes

Change Sheet

Plan Distribution

1.2 Introduction

1.3 Objective and Scope

Purpose

Objectives

1.4 Assumptions

Events included

Events excluded

Priorities

Support commitments

1.5 Responsibilities

Plan preparation/maintenance

Emergency chain of command

Operations supervisor

Shift supervisor

1.6 Strategy

Emergency response

Backup operations

Recovery

Part Two-Preparatory Actions

2.1 Personnel

Complete listing of assigned personnel with address, phone number, etc.

Emergency notification roster(s)

Team Composition

Recovery Team A

Recovery Team B

2.2 Data

On-site inventory

Off-site inventory

How/when rotated

Critical files needed for backup site processing

2.3 Application Software

On-site inventory

Off-site inventory

How/when rotated

2.4 Hardware and System Software

Inventory list

2.5 Communications

Current on-site requirements

Requirements for backup site(s)

2.6 Supplies

List of critical supply items with all necessary information (e.g., stock numbers for ordering)

List of vendors who provide supplies

(if appropriate)

List/location of supplies needed for backup site processing

2.7 Transportation

Requirements for recovery operations/backup site Procedures for emergency transportation

2.8 Space

Current site requirements (layout of facility)

Backup site space available, (by site if multiple sites involved)

2.9 Power and Equipment

Current site requirements

Backup site requirements

2.10 Documentation

On-site inventory

Off-site inventory

How/when updated

List/location of critical documentation needed

for backup site processing

2.11 Test Plans

Plan A

Plan B

Part Three-Action Plan

3.1 Emergency Response

Scenario 1

Scenario 2

Scenario n

3.2 Backup Operations

Scenario 1

Scenario 2

Scenario n

3.3 Recovery Actions

Scenario 1

Scenario 2

Scenario n

COMMENTS/REVISIONS

Technical publications under the Information Resources Management (IRM) Standards and Guidelines Program (MCO 5271.1) are reviewed annually. Your comments and/or recommendations are strongly encouraged.

IRM Tech Pub Name:

IRM- - (Number) Date of Tech Pub:

COMMENTS/RECOMMENDATIONS:

Name/Rank: (optional)

Unit: (optional)

Mail To: CG MCCDC
Requirements Division (C44)
3300 Russell Road
Quantico, VA 22134-5001