NATL INST. OF STAND & TECH R.I.C.
A11103 439020

NIST
PUBLICATIONS

NISTIR 4359

DOMESTIC DISASTER RECOVERY PLAN FOR PCs, OIS, AND SMALL VS SYSTEMS

U.S. Department of State
Bureau of Diplomatic Security

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

QC
100
.U56
#4359
1990
C.2

NATIONAL INSTITUTE OF STANDARDS &
TECHNOLOGY
Research Information Center
Gaithersburg, MD 20899

DATE DUE

Demco, Inc. 38-293

NISTIR 4359

DOMESTIC DISASTER RECOVERY PLAN FOR PCs, OIS, AND SMALL VS SYSTEMS

U.S. Department of State
Bureau of Diplomatic Security

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

August 1990

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents a disaster recovery methodology developed by Advanced Information Management, Inc., under contract to the U.S. Department of State. This NISTIR contains the Domestic Disaster Recovery Plan for PCs, OIS, and Small VS Systems.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this methodology. However, as this material may be of use to other organizations, the report is being reprinted by NIST to make it publicly available and to provide for broad dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the U.S. Department of State and Advanced Information Management, Inc., for their permission to publish this report.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, National Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

United States Department of State
Bureau of Diplomatic Security

Domestic Disaster Recovery Plan for PCs, OIS, and Small VS Systems

December 1988

U.S. DEPARTMENT OF STATE
DOMESTIC DISASTER RECOVERY PLAN
FOR PCs, OIS, AND SMALL VS SYSTEMS

CONTENTS

U.S. DEPARTMENT OF STATE
DOMESTIC DISASTER RECOVERY PLAN
FOR PCs, OIS, AND SMALL VS SYSTEMS

I. INTRODUCTION

No computer system is exempt from potential failure. Whether due to a natural disaster such as fire, or mechanical failure such as a hard disk crash, the loss of your data processing support and perhaps some critical information is a possibility for which you must prepare. You must have some way to recover critical records and to continue your work. This disaster recovery plan, properly executed, will provide that capability.

OMB Circular A-130, "Management of Federal Information Resources," requires the development of contingency plans by end-users of computer applications. This plan is designed to meet that requirement and should require less than two hours to complete. It will give you a known way to return quickly to operation should your system fail. You may wish to include more than one computer in this plan. If you have similar stand-alone computers that require the same backup strategy, data backup, and interim processing, this plan can be adapted to the entire group. When your plan is completed, all personnel involved in the recovery efforts should be given a copy.

II. PLAN DEVELOPMENT

A. Criticality Assessment

The length of time that your system can be out of operation before the impact is unacceptable (maximum acceptable delay) forms the foundation needed to establish an effective plan. Factors to consider are:

- Impact on the operation (i.e., lowered employee productivity, inability to respond to operational needs, etc.)

- Additional cost of overtime pay necessary to catch up
- The morale of your office/Bureau and the image of the Department

Accurate determination of the maximum acceptable delay provides the baseline for recovery planning. When this is known, it will help determine your backup strategy (i.e., whether a standby system is required).

B. Backup Strategy

Standard vendor hardware maintenance agreements will cover system breakdowns but will not cover loss due to fire or other disasters. If after consultation with your vendor, your equipment is declared unsalvageable, replacements may be ordered by your executive office through A/ISO/USS.

In the event timely repair or replacement of computer equipment cannot be concluded, alternative arrangements must be made:

- Manual processing including the use of typewriters for the drafting of cables and memos
- The use of reciprocal agreements that would provide you the use of another office's equipment until your service is restored. Reciprocal agreements can be concluded with another office in the same Bureau or with another Bureau which uses similar equipment. The computer at the backup site should be tested to ensure that your disk drives can be accommodated and that the operating systems are compatible. In addition, an actual test of the system will verify whether there is enough memory to accomodate shared processing.

The responsibility of relocating your replacement equipment if your room or building becomes unusable rests with the executive director of your Bureau in coordination with the General Services Administration.

C. Data Backup

It is critically important that the right data be available. The proper schedule for backing up your system is based on the timeliness of your records and the effort required to reenter data.

"System Security Standard IV", Security Standards for Unclassified Automated Information Systems in the United States, discusses the importance of an effective software and data file backup program. You should consider how long it would take to bring a two-day old file up-to-date. How long for a three-day old file? As you ask these questions, you will develop an understanding of how often you need to do backups. Balance the time it takes to back up your files with the need you have for current information. Based on that trade-off, determine the most effective backup schedule.

It is necessary to determine a safe place for storage of the backup files. A general rule is that the backup files should be a sufficient distance away from the original files so that a disaster that impacts the original files will not also impact the backup files. For example, if you are keeping your backup files in a storage area close to your equipment, a fire will probably destroy both. It is best to store your files (labeled with date of backup, highest security classification, identification of contents, operator initials, and expiration date) in another section of your Bureau, away from the central processing unit. If no secure storage area is available within your Bureau, storage areas in other Bureaus should be investigated. All files must be stored in United States Government facilities. Forms and other specialized supplies should also be maintained in a backup storage location. Should your records contain classified, controlled or sensitive information, special precautions, e.g. storage in an approved security container, must be taken. Please refer to "System Security Standard 1, "Security Standards for Classified Automated Information Systems in the United States" and "System Security Standard IV", Security Standards for Unclassified Automated Information Systems in the United States, for further guidance in this area. Unclassified files must be stored in a room with a DS approved lock.

In addition, it may be appropriate to store backup files in two places; one close by, in case of simple equipment failure or accidental erasure of files, and one further away in case of large scale disasters,

such as fire or water damage. Files that are kept close at hand are typically used for convenience rather than backup purposes.

Do not overlook the possible need to have source data available so that you can re-create electronic records that might have been lost due to the outage. There will be records created after the last backup for which there may not be duplicates. Should you be able to re-create this information from paper records? If you cannot arrange for re-creation, you should reconsider the frequency of record backup so as to minimize the impact of lost records.

D. Interim Processing

The need for interim processing capability will be based on two factors: The criticality of your processing (how long you can remain without ADP support) and your arrangements to recover from a disaster. Plans must be in place to allow your department to continue operations on a limited basis until adequate ADP support can be restored. This may include use of personal computers, sharing of word processors with others, or manual operations. At a minimum, the interim plan should allow critical business functions to continue and provide a means to rapidly recover word and data processing capabilities.

III. PREPARING FOR A DISASTER

To carry out the strategy that has been developed in the previous sections, several key functions must be performed. These are normally associated with the positions of the Disaster Recovery Manager and the System Administrator. Depending on the size of the organization, the positions may be the same person:

Disaster Recovery Manager (DRM) is responsible for:

a. Keeping the disaster recovery plan current

b. Declaring a disaster and supervising the recovery process

c. Providing the State Department Information Systems Security Office (DS/ST/ISS) with a short After-Action Report on the disaster and the recovery

The System Administrator is responsible for:

a. Keeping the interim operating plan current

b. Deciding when to contact the DRM for initiating the recovery process

c. Providing the DRM with a short After-Action Report on the disaster recovery efforts

To effectively accomplish the tasks necessary at the time of an emergency, there are several specific items that will be of great assistance:

- Notification Lists. The names and phone numbers of the personnel involved.

- Inventories. It is important to know what is needed and on hand for backup operations. Inventories are necessary for the following:

  . Equipment

  . Software

  . Data

  . Supplies and Materials

  . Transportation

These may be simple lists of only a few items or they may be more complex and require word processing support.

IV. DISASTER RECOVERY PLAN

The Disaster Recovery Plan, Attachment A, should be completed and kept up to date as the situation changes. A copy of the blank plan should be kept for updating individual pages and the document should be typed for ease of reading.

ATTACHMENT A

DISASTER RECOVERY PLAN

DISASTER RECOVERY PLAN
FOR

_____

Current as of

_____

Prepared by:

_____

CONTENTS

CHAPTER I

OVERVIEW

A. INTRODUCTION

The Disaster Recovery Plan has been prepared to define the procedures and instructions for dealing with contingency situations that may render the computer support inoperative.

This plan is divided into five chapters: I. Overview, II. Emergency Responses, III. Backup Operations, IV. Recovery, V. Maintenance, VI. Testing. Each chapter contains a narrative section plus any appendixes. The narrative sections are not expected to change frequently, but the appendixes will change because they contain more dynamic data.

B. UPDATING THE PLAN

Changes are expected on a continuing basis. Consequently, it is important to note all changes as received and to record the actions as listed in Appendix I-A, Record of Updates.

C. SAFEGUARDING THE PLAN

While this plan does not contain classified information, it is advisable that the information not be distributed indiscriminately and be limited to those with a need to know. A copy should be stored in the off-site storage location.

D. RESPONSIBILITIES

The Disaster Recovery Manager (DRM) is responsible for keeping the plan current, declaring a disaster, supervising the recovery process, and providing information to a higher authority using Appendix I-B, After-Action Report.

The System Administrator is responsible for keeping interim processing plans current, providing emergency response actions, and informing the DRM as necessary.

The names and phone numbers of the DRM, the System Administrator, and other key people are listed in Appendix I-C, Responsible Individuals.

E. CONCEPT OF DISASTER RECOVERY

In the event of a disaster affecting the computer capability, an alternate processor will be identified, and the necessary data and previously saved software will be obtained and loaded onto the system.

To provide this capability, backup data and software will be recorded and maintained at an off-site location not subject to the same potential disaster. The backup data and software requirements and locations are contained in Appendix I-D, Backup Data Procedures.

F. ACTION LOG

During a recovery it is easy to overlook a key element in the backup and recovery process. Appendix I-E, Action Item Checklist, contains a checklist of necessary actions. In addition a chronological log of specific actions should be kept.

APPENDIX I-A

RECORD OF UPDATES

CHANGES MADE

Page #	Action Taken	Date	Name of Person Updating	Updates Distributed To

APPENDIX I-B
AFTER-ACTION REPORT

Site	Date of Occurrence	Date of Report

1. Describe Disaster

(Briefly describe the events that led to Contingency Implementation.)

2. Describe Contingency Operations

(Briefly describe how operations were returned to normal conditions. Include approximate time to recover.)

Name of Reporter: _____

APPENDIX I-C

RESPONSIBLE INDIVIDUALS

DISASTER RECOVERY MANAGER

Name: _____

Phone: (Office) _____

(Home) _____

Alternate Disaster Recovery Manager: _____

Phone: (Office) _____

(Home) _____

SYSTEM ADMINISTRATOR

Name: _____

Phone: (Office) _____

(Home) _____

Alternate System Administrator: _____

Phone: (Office) _____

(Home) _____

VENDOR SUPPORT

Company Name: _____ Site No. _____

Phone: (Office) _____

APPENDIX I-D

BACKUP DATA PROCEDURES

Back up of files and records will be made no less than every _____ days. Back up usually conducted on _____.

Backup data and software is located at:

Building _____

Address _____

Room Number _____

Stored In/On _____

City _____

State _____ Zip _____

Phone # _____

_____ is responsible for backup procedures and can be reached at (Office) ___ - ___ - _____ and (Home) ___ - ___ - _____.

APPENDIX I-E

ACTION ITEM CHECKLIST

Action	Date/Time	Initials
Assess situation	_____	_____
Emergency determined; begin recovery operations	_____	_____
Notify all users	_____	_____
Notify alternate equipment provider	_____	_____
Get backup data/software	_____	_____
Begin Interim Processing	_____	_____
Implement backup equipment	_____	_____
Load software	_____	_____
Load data	_____	_____
Initiate system	_____	_____
Check system functions	_____	_____
Check backup data status (how current)	_____	_____
Update data if needed	_____	_____
Check system operation	_____	_____
Begin backup operation	_____	_____
Recovery complete, return to normal processing	_____	_____
File report with ISS	_____	_____

CHAPTER II
EMERGENCY RESPONSE

A. PURPOSE

The purpose of this chapter is to prescribe the initial actions to be taken in the event of an emergency.

B. CONCEPT OF EMERGENCY RESPONSE

The following list provides emergency phone numbers for use during a crisis:

EMERGENCY CALLS

Bomb Threats or Other Danger Requiring Immediate Action:

Emergency Medical Assistance:

Fire:

Police:

Safety Office:

The Safety Division (A/OPR/SAF) distributes the "Occupant Emergency Plan" which provides instructions for actions to be taken in case of fire, bomb threats, or disaster emergencies. Copies of this emergency plan are available through your executive office or by contacting the Safety Division.

In addition, the Fire Safety and Hazard Control Division (A/FBO/FIRE) distributes pamphlets on fire safety and prevention. Examples of these booklets are: "Understanding Portable Fire Extinguishers" and "About High Rise Fire Safety." A publication entitled "Guidelines for Fire Protection of Essential Electronic Environments" is geared toward larger data processing centers.

C. FAILURE ASSESSMENT

It is imperative that an assessment be made as quickly as possible of the probable time to repair and restart the system. This may be quite obvious or may require that the customer engineer be called to obtain an accurate estimate. As soon as the assessment is made, the DRM should be notified so that a decision on recovery implementation can be made.

To accomplish Failure Assessment effectively, it is necessary to have available lists of equipment, software, and data, Appendix II-A.

D. AFTER-ACTION REPORT

An After-Action Report, Appendix I-B, should be filed with the DRM two weeks after recovery of disaster.

APPENDIX II-A

INVENTORIES

(Use additional sheets if required)

EQUIPMENT COVERED

List hardware maintained by your office:

Model #	P. Order #	Item -	Serial #	Vendor	Location

SOFTWARE COVERED

List critical software (operating system and applications). What each supports:

ID	Name	Version	Vendor	Language	Person Responsible

DATA COVERED

List database and files. This may include data for any function. (e.g., Passport database, form letters, accounting records, etc.)

ID	Name of Data	Owner	Description	Backup Frequencies

SUPPLIES AND MATERIALS FOR BACKUP OPERATIONS

As of: _____ (Date) Last Inspected: _____ (Date)

Description	Quantity Required	Quantity on Hand

TRANSPORTATION

Vehicle Number	Passenger Capacity	Load Capacity

CHAPTER III
BACKUP OPERATIONS

A. PURPOSE

The purpose of this chapter is to provide instructions for the activation of the backup operations plan.

B. DISASTER RECOVERY CONCEPT

There are three potential techniques for recovery: Replacement of Equipment, Mutual Assistance, or Manual Processing. The approach selected should be indicated here and the details placed in Appendix III-A, Backup Concept:

- Replacement of Equipment
- Mutual Assistance
- Manual Processing

C. INTERIM PROCESSING

In some cases it may be necessary to implement interim processing for specific critical applications. Each such application is detailed in Appendix III-B, Interim Processing Requirement.

D. AFTER-ACTION REPORT

An After-Action Report, Appendix I-B, should be filed with the DRM two weeks after recovery of disaster.

APPENDIX III-A
BACKUP CONCEPT

If a disaster occurs that indicates that the system will not be available for more than _____ (days/hours), the DRM or other authorized person will declare that the disaster plan should be implemented. This should be indicated on the Action Item Checklist (Appendix I-E).

If system restoration is necessary, it will be accomplished by (check and complete the appropriate plan):

____ Replacement Equipment:

Responsible Individual _____

Phone: (Office) _____

(Home) _____

Equipment will be shipped to:

_____

_____

_____

Equipment will be available within _____ (days/hours) of notification.

_____ Use of equipment of an organization with whom a mutual assistance agreement has been negotiated:

Name of Organization _____

Responsible Individual _____

Phone: (Office) _____

(Home) _____

Building _____

Address _____

Room Number _____

City _____

State _____ Zip _____

Type of equipment

Vendor _____

Model _____

Operating System and Release Number _____

Mode of Operation: Shared _____

Dedicated _____

Number of workstations available for use _____

Number of printers available for use _____

Compatibility of application hardware, i.e., memory size, disk format, graphics and magnetic media compatibility _____

Equipment is approved for unclassified _____, LOU _____, Confidential _____, and Secret _____ processing.

Equipment can be utilized within _____ (days/hours) of notification.

APPENDIX III-B

INTERIM PROCESSING REQUIREMENT

APPLICATION: _____

Method of Accomplishment:

_____ Manual

_____ Backup Automation Support

Description:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

(Repeat as Necessary)

CHAPTER IV
RECOVERY

A. PURPOSE

The purpose of this chapter is to establish procedures for restoring normal computer operations.

B. CONCEPT OF RECOVERY

Regardless of how well planned and executed the backup operations are, when the computer center is destroyed, they will be something less than optimal. Restoration of the primary facility will therefore be of prime importance.

Because of the wide range of potential situations, it will be necessary to plan the recovery based on the condition of equipment and facilities at the time of the disaster. The approach will be to individually assess the recovery potential of specific elements and to combine these elements into a recovery plan. The plan outline is contained in Appendix IV-A, Recovery Plan Outline.

C. INVENTORIES

The inventories contained in Appendix II-A will be equally useful for recovery planning.

D. AFTER-ACTION REPORT

An After-Action Report, Appendix I-B, should be filed with the DRM two weeks after recovery of disaster.

APPENDIX IV-A

RECOVERY PLAN OUTLINE

I. EQUIPMENT

Item	Serial #	Repair	Replace	Available Date

II. SOFTWARE/DATA

ID	Backup Storage	Date of Backup	Update Needed	Available Date

III. **FACILITY**

Repairs Needed	Performed By	Available Date

IV. **OTHER ACTIONS NECESSARY**

(Communications, Personnel, etc.)

CHAPTER V

MAINTENANCE

A. PURPOSE

The purpose of this chapter is to prescribe specific actions necessary to ensure that this plan is kept up-to-date.

B. CONCEPT OF MAINTENANCE

Appendix V-A, Maintenance Index, lists the maintenance actions necessary. Space is provided to assign responsibility, frequency of action, and date of accomplishment.

APPENDIX V-A

MAINTENANCE INDEX

Section	Responsibility		Frequency	Date Last Updated
	Office	Name		
I-C Notification Lists	_____	_____	As required	_____
I-D Backup Procedures	_____	_____	Quarterly or as changed	_____
II-A Inventories	_____	_____	As changed	_____
III-A Backup Concept	_____	_____	As changed	_____
III-B Interim Processing	_____	_____	As changed	_____
IV-A Recovery Plan	_____	_____	As changed	_____
Overall	_____	_____	Quarterly	_____

CHAPTER VI

TESTING

You may wish to perform operational testing at your selected backup facility once or twice a year.

Each testing session should last for no more than one day and should be cleared in advance with both system managers. Before testing you should consult with your equipment vendor to insure that proper procedures are followed when transporting and reloading your media.

Testing shold be performed in the same mode of operation (shared or dedicated) as provided for in the mutual assistance agreement.

Operational testing is beneficial because it identifies incompatibilities between the two systems. For this reason, it is important that the system managers at both data processing sites receive advance notice of software and hardware changes.

NIST-114A
(REV. 3-89)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4359

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
AUGUST 1990

4. TITLE AND SUBTITLE
Domestic Disaster Recovery Plan for PC's, OIS, and Small VS Systems

5. AUTHOR(S)
US Department of State

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)
Reprinted by permission of the U.S. Department of State, Office of Information Security, Washington, DC 20520 and the Advanced Information Management, Inc. Woodbridge, VA 22192

10. SUPPLEMENTARY NOTES

[ ] DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The Domestic Disaster Recovery Plan for PCs, OIS, and Small VS Systems provides a methodology for developing a disaster recovery plan for small computer systems. It describes how a plan is to be developed, including, specifically: determination of the criticality of processing requirements, backup strategy, data backup, and interim processing. The assignment of responsibilities for key computer personnel are also discussed. Finally, the model Disaster Recovery Plan is presented. It is organized into six chapters: I. Overview, II. Emergency Response, III. Backup Operations, IV. Recovery, V. Maintenance, and VI. Testing.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)
disaster recovery, contingency planning, computer security, ADP security, automated information systems security

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
37

15. PRICE
A03

ELECTRONIC FORM