

DISASTER RECOVERY PROCEDURE

VIRGINIA SURETY NETWORK

OBJECTIVE	4
IDENTIFICATION OF CRITICAL USERS	5
WHEN ONE SERVER IS USED AS THE TEMPORARY SOLE FILE SERVER	5
WHEN NO FILE SERVERS ARE AVAILABLE (USING COMMUNITY PCs)	5
CRITICAL USERS	5
VSC1 File Server	5
VSC2 File Server	6
OVERVIEW OF RESPONSIBILITIES	7
ADMINISTRATION CONTACT	7
UNIT MANAGERS	7
NETWORK USERS	7
USER ADMINISTRATOR	8
HELP DESK	8
IT SUPPORT	8
AIS DEVELOPMENT	9
EMERGENCY WORKSTATIONS/TERMINALS	10
COMMUNITY WORKSTATIONS	10
HERITAGE	10
AMEGA/DISPLAYWRITE	11
DISASTER RECOVERY PROCEDURE	12
When the Servers Become Non-Functional	12
WHEN THE NETWORK FAILS	13
1. ALERT APPROPRIATE PEOPLE	13
2. IT SUPPORT EVALUATES/RESOLVES FAILURE	14
3. ACTIVATE SOFTWARE ON DESIGNATED COMMUNITY PCs	14
4. INFORM NETWORK USERS OF COMMUNITY PCs	14
5. INFORM NETWORK USERS OF TEMPORARY SETUP OF NETWORK	14
WHEN THE NETWORK BECOMES FUNCTIONAL	15
1. ALERT APPROPRIATE PEOPLE	15
2. TEST NETWORK GENERIC APPLICATIONS	16
3. TEST NETWORK PRINT QUEUES	16

4. TEST CUSTOM APPLICATIONS	16
5. RESTORE SOFTWARE TO NETWORK	16
6. IT SUPPORT RE-ESTABLISHES NETWORK	16
7. RE-SET NETWORK CONNECTION FOR COMMUNITY PCs	16
8. INFORM USERS THAT THE NETWORK IS AVAILABLE	16
IMPORTANT INFORMATION	17
KEY PEOPLE	17
1. USER ADMINISTRATOR	17
2. ADMINISTRATION CONTACT	17
3. AIS DEVELOPMENT CONTACTS	17
4. HELP DESK	17
5. IT SUPPORT	17
6. NETWORK CONTACT USERS / USER GROUPS	17

OBJECTIVE

Data and equipment functionality are essential to any organization. They are directly related to employee functionality and deeply affect financial health and competition. A breakdown in either of these could prove disastrous. If a system is structured well, it is rare that its functionality ceases. For this reason, people tend to expect the overall endurance of a system to be perpetual.

Unfortunately, unforeseen system failures or damage can occur for various reasons. The ability to recover from lost or damaged software and hardware is extremely crucial and necessary. It is additionally crucial that the recovery is as swift and efficient as possible.

Therefore, a Disaster Recovery Procedure has been developed to assist in the stability of the system. Ideally, this procedure will never need to be carried out. However, it is highly important that all parties involved are familiar with the recovery process. This familiarity will ensure the swift and efficient return to functionality of the system.

This Disaster Recovery Procedure document outlines the following aspects:

- **Identification of Critical Users**
- **Overview of Responsibilities**
- **Emergency Workstations**
- **Specific Disaster Recovery Procedures**
- **Important Information (key people)**

With this goal in mind, the information on the following pages is of the utmost importance.

Thank you, in advance, for taking the time to become thoroughly familiar with this procedure.

IDENTIFICATION OF CRITICAL USERS

The critical users will have first priority to utilize any temporary setup that is available during a Network failure.

The critical users consist of two groups as follows:

Group 1: This group will share half of all available Network IDs or community PCs and includes...

- **Lead Administrative Assistants from each department**
- **Submission Processors**
- **Policy Processors**

Group 2: This group will use the remaining available Network IDs or community PCs and includes...

- **Underwriting Department Managers**
- **Claims Department Head**
- **Administration Department Head**

WHEN ONE SERVER IS USED AS THE TEMPORARY SOLE FILE SERVER

If a server is temporarily functioning as the sole server during a network failure or a disaster, the critical users will be given access to the network before all other users. If additional Network IDs are feasible (100 is the maximum), affected non-critical users may be setup to utilize the server. Otherwise, the non-critical users will share the community PCs (see Section V for locations).

WHEN NO FILE SERVERS ARE AVAILABLE (USING COMMUNITY PCs)

If no file servers are available for use, the community PCs will be the solitary means of operation. In this situation, the critical users will share community PCs. Non-critical users will await the repair of the Network (see Section III for locations).

CRITICAL USERS

VSC1 File Server

Group 1

USER NAME	LOCATION
Joy Bahar	2
Whoopi Goldberg	2
Barbara Walters	2
Elisabeth Hasselbeck	2
Tina Chu	2
Julio Jones	2

VSC1 File Server (continued)

Group 2

USER NAME	LOCATION
Willie Mays	3
Peter Cottontail	3
Rebecca Howell	3
Chelsea Lately	3
Susie Snowflake	3
Robert Collins	3

VSC2 File Server

Group 1

USER NAME	LOCATION
Bob Hope	3
Bing Crosby	3
Betty White	3
George Burns	3
Paul George	3
John Ringo	3

Group 2

USER NAME	LOCATION
Wilma Flintstone	3
Betty Rubble	3
Jada Pinkett	3
Winnie Mandela	3
Where U. Been	3
Long Tyme Nocee	3

OVERVIEW OF RESPONSIBILITIES

All Network users are responsible for performing and cooperating with certain safety measures. All of these safety measures ensure minimal data loss in case of a Network disaster and should be practiced on a daily basis.

The Network safety measures are as follows:

- **Batched Data Entry:** Data will be entered in batches and checked after every 5 entries. Also, paper documents will be kept available until after the scheduled Network backup.
- **Periodic Saving of Documents:** All documents, reports, and spreadsheets need to be saved every few minutes. As such, MS Word, Crystal Reports, and MS Excel will be setup to automatically save data every 5 minutes.
- **Scheduled Network Backups:** Currently, all Network data and software are backed up on a regular basis. This will continue to be the case. Custom application data is backed up every afternoon. All files are backed up every evening.

The following is a brief description of the responsibilities of the various parties of the Network:

ADMINISTRATION CONTACT

- Ensure that the Unit Managers understand the concept of batched data entry, periodic document saves, and Network backups.
- Emphasize the role the safety measures play in guarding against data loss during Network disasters.
- Explain the importance of being familiar with the steps to be taken in case of a Network disaster (see Section VI for steps).

UNIT MANAGERS

- Ensure that direct reports understand the concept of batched data entry, periodic document saves, and Network backups.
- Emphasize to direct reports the role that the safety measures play in guarding against data loss during Network disasters.
- Explain to direct reports the importance of being familiar with the steps to be taken in case of a Network disaster (see Section VI for steps).

NETWORK USERS

Practice and understand the concept of batched data entry, periodic documents saves, and Network backups.

Overview Responsibilities - NETWORK USERS (continued)

Understand and appreciate the role that safety measures play in guarding against data loss during Network disasters.

Be familiar with the steps to be taken in case of a Network disaster (see Section VI for steps).

USER ADMINISTRATOR

Have thorough knowledge of the Disaster Recovery Procedure and the steps to be taken in case of a Network disaster.

Assist Administration Contact and the user community in becoming familiar with the steps to be taken in case of a Network disaster.

Encourage Network users to practice batched data entries.

Conduct afternoon backups of Custom Application data.

When the Network fails, immediately contact the Help Desk, Administration Contact, Network Contact Users, and AIS.

Act as the contact person for IT Support, AIS, and Network users during Network failures.

HELP DESK

The Help Desk is the first and a very crucial step in the disaster recovery process. The Help Desk's responsibilities include the following:

- Obtain vital information regarding the Network name, error messages and/or symptoms and the time of the problem.
- IMMEDIATELY relay information to IT Support.

IT SUPPORT

- Provide input regarding safeguards against Network disasters including the Disaster Recovery Plan.
- Have thorough knowledge of the steps to be taken in case of a Network disaster.
- Oversee nightly, monthly, yearly and special backups.
- Determine the cause of a Network failure and remedy the problem.
- Once Network failure has been corrected, restore the Network to its normal condition.

AIS DEVELOPMENT

The responsibility of AIS is to work in conjunction with the User Administrator and IT Support to safeguard against Network disasters. However, if a disaster does occur, AIS works closely with the User Administrator and IT Support in carrying out the various disaster recovery steps as appropriate. The responsibilities of AIS are as follows:

- Develop and maintain and Disaster Recovery Procedures for the user community and IT Support.
- Publish the Backup and Disaster Recovery Procedures for the user community and IT Support.
- Closely monitor the condition of the Network and convey the need for repairs to IT Support.
- Assist User Administrator and IT Support during a Network disaster as needed.

Adherence to the above responsibilities is very essential toward achieving minimal data loss and a prompt recovery if a Network disaster occurs.

EMERGENCY WORKSTATIONS/TERMINALS

If a file server becomes nonfunctional, IT Support will usually reconfigure the one functioning server as the temporary sole file server. However, in the interim or if both file servers become nonfunctional, there are community PCs and terminals available for use in case of a Network failure.

COMMUNITY WORKSTATIONS

There are community workstations on the Network which consists of a “fully-loaded” hard drive. What’s a fully-loaded hard drive? It’s just a term that IT Support uses to describe a hard drive that has the basic software needed to carrying out day-to-day office work. This includes the following...

- **Microsoft Word**
- **Microsoft Excel**
- **Microsoft Access**
- **Crystal Reports**

Using these applications, you can continue to generate basic office communication (letters, documents, reports, etc.). These workstations are located in the following areas:

- **Fax Room – 2nd Floor**
- **Admin Area – 2nd Floor NW corner**
- **Claims Area – 3rd Floor SE corner**
- **Workers’ Compensation Area – 3rd Floor NW corner**

Looking at the list of software listed above (MS Word, MS Excel, etc.), you’ll notice that our custom applications are missing. These applications are essential since they are used to track our insurance packages, and process our claims. No need to worry, though. As a precaution, all custom applications and insurance data are backed remote servers. These servers are located in another part of the country and can be accessed via terminals that will be discussed in the following section.

HERITAGE

There are two terminals that allow access to Heritage. Excluding a company-wide or building power outage, these terminals can be used in case of a Network failure.

These terminals are located in the following areas:

- **Claims Area – 3rd Floor SE corner**
- **Workers’ Compensation Area – 3rd Floor NW corner**

AMEGA/DISPLAYWRITE

There is one terminal that allows remote access to Amega/Displaywrite. There is also a printer used for Amega/Displaywrite that is independent of the Network. Excluding a company-wide or building power outage, this terminal and printer can be used in case of a Network failure.

This particular terminal and printer are located in the **Copy Room on the south end of the 2nd floor**. Additionally, there are **terminals on the 16th floor** that will be available during a network failure.

Using the community workstations and the terminals mentioned above ensures that VSC can continue to carry out its essential functions following a disaster or network failure.

DISASTER RECOVERY PROCEDURE

The functionality of the VSC Network depends on the file servers. This Disaster Recovery Procedure has been developed as a guideline in the event that one or both network servers become non-functional. In case of a network failure (due to disaster, power outage, equipment failure, etc.), certain steps need to be taken concerning the various data utilized on the VSC Network.

The following is an outline that describes how to respond during a network failure.

When the Servers Become Non-Functional

- Alert the Appropriate People
- IT Support Evaluates/Resolves Failure
- User Administrator and AIS activate Software on Community PCs
- User administrator Informs Network Users of Community PCs
- User Administrator Informs Network Users of Temporary Setup of Network*

When the Servers Become Functional

- Alert the Appropriate People
- AIS/VSC Test Network Generic Applications
- AIS/VSC Test Network Print Queues
- AIS Tests custom Applications
- IT Support Restores Software to Network*
- IT Support Re-establishes Network to its Original State*
- User Administrator and AIS Re-set Network Connection to Community PCs
- User Administrator Informs Users Network is Available

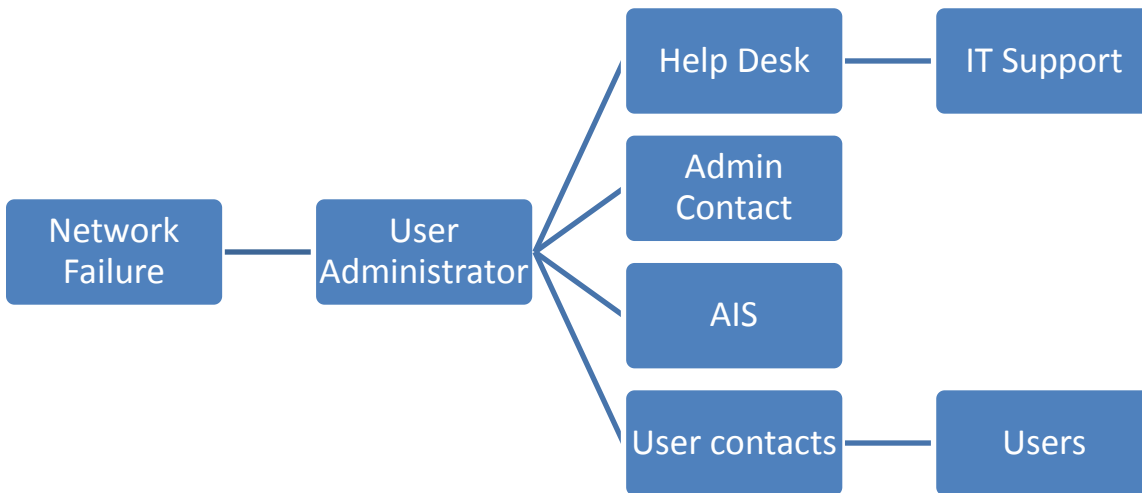
**Performed Only if Applicable*

➡ DETAILED DISASTER RECOVERY STEPS BEGINN ON FOLLOWING PAGE ➡

WHEN THE NETWORK FAILS

1. ALERT APPROPRIATE PEOPLE

When the network fails, key people must be alerted immediately. These key people are notified in the following manner:



The following is an explanation of the above diagram:

a) HELP DESK

The User Administrator immediately contacts the Help Desk at extension 50-8511, and provides them with as much information as possible. The Help Desk then contacts IT Support at extension 50-3774

b) ADMINISTRATION CONTACT

After contacting the Help Desk, the User Administrator promptly notifies the Administration Contact of the network failure. The Administration Contact is given an overview of the situation and is assured that the Help Desk has been contacted.

c) AIS CONTACTS

At this point, the User Administrator should notify the AIS contact(s) at extension 50-4765. The User Administrator provides AIS with as much information as possible. At this point, AIS assists the User Administrator and IS Support where possible.

d) NETWORK CONTACT USERS

The User Administrator alerts the Network Contact Users that the server is down and that they need to turn their PCs *off*. The User Administrator also informs the Network Contact Users that the Disaster Recovery Procedure is officially in effect, and that Heritage and Amega terminals are available for immediate use*. At this point, each Network Contact User immediately relays this information to the users in their respective user group.

2. IT SUPPORT EVALUATES/RESOLVES FAILURE

IT Support proceeds by evaluating the basis of the network failure. Once the cause(s) has been determined, IT Support attempts to remedy the situation. If feasible, IT Support will reconfigure one file server to temporarily operate as the sole file server.

3. ACTIVATE SOFTWARE ON DESIGNATED COMMUNITY PCs

At this point, the User Administrator and AIS activate designated community PCs to be used in the interim. These PCs are located in the following areas:

2nd Floor

- Fax Room
- Admin Area – NW corner

3rd Floor

- Claims Area – SE corner
- Workers' Compensation Area – NW corner

The stand-alone PCs are activated. Now, all software (MS Word, MS Excel, MS Access, and Crystal Reports) is available for use.

4. INFORM NETWORK USERS OF COMMUNITY PCs

Once the stand-alone software has been activated, the User Administrator and AIS notifies Network Contact Users of the availability of the community PCs. In turn, the Network Contact Users notify the users in their respective group.

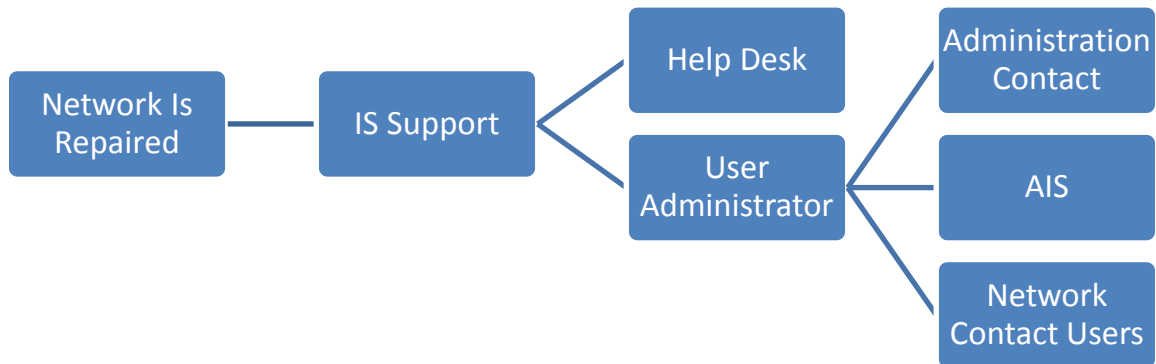
5. INFORM NETWORK USERS OF TEMPORARY SETUP OF NETWORK

This process is carried out only if IT Support reconfigured a file server to operate as the sole file server. When IT Support is ready to implement this temporary setup, they immediately notify the User Administrator. The User Administrator then apprises the Network Contact User, who then relays the information to the users in their respective user group.

WHEN THE NETWORK BECOMES FUNCTIONAL

1. ALERT APPROPRIATE PEOPLE

Once the network failure is remedied, notification is then carried out in the following manner:



The following is an explanation of the above diagram:

a) **HELP DESK**

IS Support will immediately contact the Help Desk at extension 50-8511. The Help Desk is then provided with as much information as possible regarding the remedy for the network.

b) **USER ADMINISTRATOR**

After contacting the Help Desk, IT Support promptly notifies the User Administrator that the network has been repaired. The User Administrator is provided with an overview of the problem and its solution.

c) **ADMINISTRATION CONTACT**

The User Administrator then notifies the Administration Contact that the Network has been repaired. The Administration Contact is given an overview of the situation.

d) **AIS DEVELOPMENT**

At this point, the User Administrator notifies the AIS contact(s) at extension 50-3147. AIS is provided with as much information as possible.

2. TEST NETWORK GENERIC APPLICATIONS

At this point, AIS and VSC will test the various software packages on the network. This will be accomplished by sitting with every user and testing each Basic Application option. Amega and Heritage access will also be tested.

3. TEST NETWORK PRINT QUEUES

AIS and VSC tests the network for the appropriate default printers and the proper print queues responses.

4. TEST CUSTOM APPLICATIONS

AIS will thoroughly test the functionality of the custom applications on the affected file server(s). Any and all discrepancies are noted. Once the custom applications are tested, the appropriate Audit Trail reports are generated.

Based on the Audit Trail reports, VSC personnel need to check the integrity of the applications' data, and any discrepancies must be carefully noted.

5. RESTORE SOFTWARE TO NETWORK

If **any** of the generic or custom applications on the network are not functioning properly, IT Support will restore it using the most recent “**nightly**” tape backup (and/or the most recent “afternoon” tape backup, if necessary).

6. IT SUPPORT RE-ESTABLISHES NETWORK

The network may have been re-configured as a temporary remedy during the failure. If this is the case, IT Support needs to re-establish the network's usual configuration before users can resume use of the network.

7. RE-SET NETWORK CONNECTION FOR COMMUNITY PCs

The User Administrator and AIS need to re-set the community PCs so that they are connected to the network.

8. INFORM USERS THAT THE NETWORK IS AVAILABLE

The User Administrator alerts the Network Contact Users that the server has been repaired and is available for use. Each Network Contact User then relays this information to the users in their respective user group.

The users can then login and utilize the Network as usual.

IMPORTANT INFORMATION

KEY PEOPLE

1. USER ADMINISTRATOR

Maria Gonzales	50-3264
----------------	---------

2. ADMINISTRATION CONTACT

Leslie Lee	50-4639
------------	---------

3. AIS DEVELOPMENT CONTACTS

Amanda Manilow	50-4765
Harry Carry	50-3982

4. HELP DESK

Gale Sayers	50-8562
-------------	---------

5. IT SUPPORT

Hay Yu	50-3774
--------	---------

6. NETWORK CONTACT USERS / USER GROUPS

Contact (Primary/Secondary)

User Groups

#1 Paula Rodriguez	50-4938
#2 Judy Boros	50-3458

Carolyn Barrett
Karen Connolly
Coral Reefs
Leslie Lee
Chris Cross
Nancy Fancy
Sheila Lake

#1 Inna Rhutt	50-4786
#2 Alice Cooper	50-4788

Christine Bacharach
Denise Cristo
Emilie Smith
Renee Topps
Marnie Fitz
Don Draper
Janis Joplin

#1 Mary Mann	50-4670
#2 Patty Kake	50-4583

Eddie Kendricks
Cindy Ireland
Esther Martin
Greg Sparks
Pam E. Lah