Contingency Planning
Phase 1 - Servers

1. In developing an appropriate computer security profile, contingency plans will be written on all critical systems. MID will begin the contingency planning process with the 15 servers we are directly responsible for. See table below for your area of responsibility.

SERVER	PURPOSE	LOCATION	CONTACT
SERVER 1	DENCAS REMOTE ANTIVIRUS CONSOLE VERITAS NET BACKUP	MID	ET3 Pierce
SERVER 01	PRIMARY COMMAND SERVER/PUBLIC STORAGE, MPERS/ FILE SERVER	MID	ET3 Gonzales
SPMS	MANPOWER	MID	DT1 Bano
SERVER 2	LAN PRINT SERVER	MID	Ms. Parrish
EXCHANGE	E-MAIL SERVER	MID	DT2 Telmo
EAS4	MANPOWER	PAYROLL	DT1 Bano
WEB SERVER	INTRANET	MID	Ms. DeMars
WEB SERVER	PUBLIC WEB	NMC SAN DIEGO	Ms. DeMars
SDI SERVER	SMART CARD	MCRD	ET3 Gonzales
WEBMAIL	OUTLOOK WEB ACCESS	MID	DT2 Telmo
DIMAXIS	DIGITAL X-RAY	MCRD	IT1 Opsteegh
FASTDATA	ACCOUNTING	MID	Ms. Parrish
CLASSIFIED MESSAGE	MESSAGE TRAFFIC	MID	IT1(SW/AW) OPSTEEGH
INCOMING MESSAGE TRAFFIC (A)	UNCLASSIFIED MESSAGES SEND/RECEIVE	MID	IT1(SW/AW) OPSTEEGH
UNCLASSIFED MESSAGE TRAFFIC (B)	MESSAGE DISSEMINATION THROUGHOUT COMMAND (CONNECTED TO NETWORK)	MID	IT1(SW/AW) OPSTEEGH

2. The idea of a contingency plan is as follows:

    a. the system crashes

    b. MID tech grabs the contingency plan

    c. and knows what to do

3. Formal format for the individual contingency plans has not yet been established. Here are some things to consider:

    a. Purpose of System – what is the purpose(s) of this particular system

    b. Impact – what is the impact to the command if this system crashes. Indicate primary users. Is a short down time OK? What could be acceptable?

    c. Inventory info – location, serial #, barcode, make/model

    d. Hardware contents – processor, hard drives, memory

    e. Software loaded – operating system, application software. Indicate where to find installation disks.

    f. POC – is there an outside party to be called for assistance? Provide info.

    g. Backup – how and when is this system backed up? Where is the backup stored? What's included in the backup?

    h. Risks and solutions – write a minimum of one paragraph addressing each of the possible risks and solutions. Include time estimates and degree of difficulty. Include possible sources for purchasing replacement parts.

4. Risks come in many forms. Write a solution for each. OK to add more.

    a. Total system loss – due to theft, fire, vandalism

    b. Motherboard, processor, or memory failure

    c. Hard drive failure

    d. Operating system failure

    e. Application failure

    f. Virus attack

g. Internal sabotage

5. Timeline.

Due Date	Task
05Jan04	Familiarize yourself with paragraphs 1 and 2 regarding the purpose and responsibilities of the contingency plan project
12Jan04	Write description of system as responses to paragraph 3. Format will be provided by Head, MID
30Jan04	Write risks/solutions as indicated in paragraph 5. Provide as much detail as someone familiar with computers, but unfamiliar with this particular system would need to recover from a catastrophe
06Feb04	Head, MID review all contingency plans
13Feb04	Develop test plan
20Feb04	Conduct test of each system contingency plan

6. This Contingency Plan project has to be a totally cooperative effort between all MID team members. All of us know something about these systems. Now is the time to document our knowledge and create a viable contingency plan. Imagine if you were the MID tech chosen to recover a broken system. You can pick up this plan and get most of your answers readily and begin a quick recovery. Write the best contingency plan you can. Each of you is very knowledgeable and now is the time to prove it with a quality document.

7. What's Next? Start making a list of other critical systems, network switches, and MID will tackle making contingency plans for those as well.

8. Any Questions? See Ms. DeMars, LTJG Kraft, and IT1 Opsteegh