Write a disaster/contingency plan. Review the materials in this chapter on disaster/contingency planning. Prepare a contingency plan for a typical home computer installation or another installation you have responsibility for. Your plan should:

1. Identify any important risks to the ongoing operation of the installation. (How likely is each risk you identified?)

2. Describe any applicable insurance that would cover replacement costs if the installation was damaged, stolen, or destroyed.

3. Identify any security vulnerability or security devices (including detectors and alarms) that apply to the installation.

4. Describe the location of media backups (including both on-site and off-site backups), detail how frequently backups are created, and specify the restoration procedures.

5. Outline the major steps necessary to get the installation operational again after any kind of disaster.

1.

Important risks to the installation's continued functioning include:

Equipment

Software media

Applications/programs

Data

Records

Proprietary programmes

Revenue lost

2.

Damage to computers, media, and data are all covered by electronic data processing (EDP) insurance. If your company relies on computers to run its daily operations, this coverage is crucial. Many of the holes in conventional business property laws regarding electronic equipment are filled by this. Typically, policies cover three types of property.

Equipment (personal computers, servers, terminals, moniters, laptops and other hardware)

Media (Disk drive, disks, magnetic tapes and other location where data is kept in your machine) (Disk drive, disks, magnetic tapes and other area where data is stored in your equipment)

Data (Software application that hold your business data and facts, concepts, or programmes as well as additional expenses related with data recovery) (Software application that store your business data and facts, concepts, or programmes as well as additional expenses associated with data recovery

3.

Security tools including security cameras and fire alarms, as well as other potential house invaders

4.

Remort backups are a critical component of your backup system. It may be pointless to make a backup of your data and keep it on the same disc as your original data. Off-site storage, or at the very least off-server storage, will continue to function even if your primary server is compromised, enabling complete data recovery. Off-site backups are essential for effective disaster recovery, whether they are stored on a physically dedicated or cloud-based server. Take backup regularly encrypted and protected.

By downloading our encrypted backup from a cloud-based server, we can restore it to a different home desktop or Central server.

5.

The primary action required to restore the installation to operation following any type of disaster:

computer room setting (secure computer room with climate control, conditioned and back-up power supply etc.)

Hardware (network, server, desktop, and laptop computers, wireless devices and peripherals) (network, server, desktop, and laptop computers, wireless devices and peripherals)

Joining up with the service provider (fibre, cable, wireless, etc.)

computer programme (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)

Data and data recovery