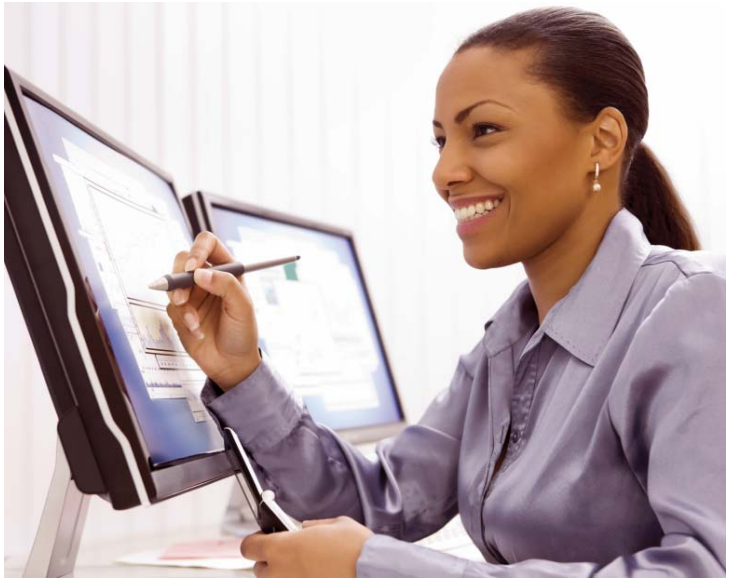
The Security Manager

October 23, 2011

Normal Duties of a Network Manager

- Responsible for the Physical LAN
  - Servers rooms and their devises
  - LAN infrastructure including wires and wireless
  - Computers, printers, scanners and other user devises
- Accountable for Information Security
  - Protect data owned by the organization
  - Protect data access
  - Restore data when lost
- Assist in Personnel Security
  - Screen employees to assure the individual is trustworthy
  - Audit computer users to discover inappropriate access to data
  - Manage all network access



Extreme Duties of a Network Manager

- Disaster Recovery Planning (DRP)
  - Analyze, plan and publish a DRP
  - Update the document periodically
  - Communicate the plan to the leaders and critical workers in the organization
- Disaster Recovery Drills
  - Conduct rehearsal monthly
  - Make improvements to the plan
  - Conduct training sessions to implement changes
- Disaster Recovery
  - Follow the plan in framework
  - Complete the recovery safely
  - Use your leadership to overcome obstacles

Skills of a Security Manager

Security managers are often highly trained server specialist and computer technicians. Then they typically excel as a LAN manager and worked their way to their current position where they are the best at anticipating and solving problems. They use checklists and procedures to accomplish their tasks since they can distribute the procedures and delegate the actual work to any skilled technician in their department.

Several DRP Procedures

- Accessing the damage to a LAN
- Making a purchase order
- Removal of broken equipment
- Wire and wireless router configuration
- Windows 2008 server installation
- Active Directory setup and maintenance
- Reinstalling server data
- Client machine imaging
- Printer and scanner setup
- Overhead projector setup

Recovering as Part of a Larger System

Our small organizational LAN may be just a fraction of the larger failure in a disaster. Each country has a system to handle those problems. In the United States of America, we have the Federal Emergency Management Agency (FEMA) that oversees the national level DRP.

Natural Disasters

Some natural or manmade disasters can be planned for and historically happen in certain regions of the world. We can study our geographical location and begin by planning for the disasters that can occur locally.

In our region, we can experience spilled hazardous materials, floods, fire, nuclear power plant emergency, terrorism, thunderstorm, tornado and winter storm. We should have different plans to respond to these emergencies. In those plans there will be common procedures.

Prepare for a Disaster

For each type of disaster, we need to create a short assessment of what we should do to safeguard our network, data and personnel. We can use a single page assessment form and our knowledge of our organization and region to develop a plan that can be accomplished.

Company Confidential

Type of Disaster	Flood
Terms	Flood watch: Flooding is possible. Flash Flood watch: Flash flooding is possible. Be prepared to move to higher ground. Flood Warning: Flooding is occurring or will occur soon, if advised to evacuate, do so immediately. Flash Floor Warning: A flash flood is occurring; seek higher ground on foot immediately.
Recommended Actions Before	Avoid building in a flood plain unless you elevate and reinforce your home. Elevate the furnace, water heater, and electric panel if susceptible to flooding. Install "check valves" in sewer traps. Construct barriers (levees, beams, floodwalls) to stop floodwater from entering the building. Seal walls with waterproofing compounds to avoid seepage.
Recommended Actions During	Listen to the radio or TV. Be aware that a flash flood could happen. Prepare to evacuate, turn off utilities at the main switch panel. Shut down all the computers correctly. Do not walk through moving water. Do not drive through moving water. Six inches of water is enough to make you fall, stall a car and loose control of the car. Two feet of water can carry a vehicle away.
Recommended Actions After	Listen to news reports to see if water is safe to drink. Avoid floodwaters, they could be contaminated by oil, gas, or raw sewage. Avoid moving water. Stay away from downed power lines and report them to power companies. Return back to the building when authorities say it is safe to do so. Stay out of the building if it is surrounded by flood water. Clean and disinfect everything that got wet. Check all equipment and go through the DRP.
Equipment Needed	Have a safety kit ready; first aid, flash lights (lots of them) etc. Floods can wipe out power and inside a server room if for some reason emergency power does not come on, flash lights are needed. After the flood, have the contract clean up team ready and in place to get everything back up to spec.
IT Department Procedures during the Event	Turn off all equipment safely. Follow the DRP correctly, fast, and effectively. Turn off the main breakers and follow supervisor instructions. If not under flash flood warning, evacuate the building and seek higher ground.
Submitted by:	Steve Smith
Date:	11-3-2006

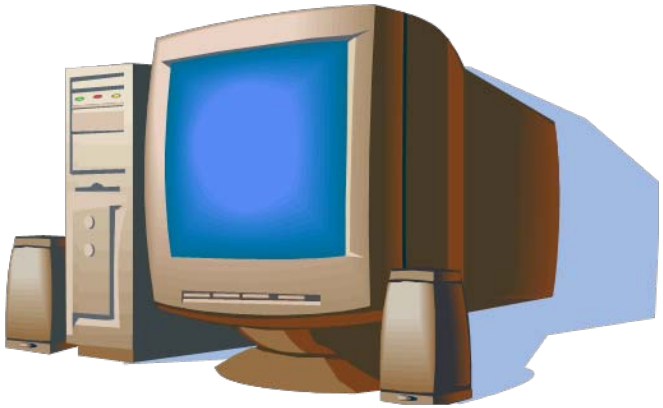
Assignment

Develop a single page assessment for the following disasters for your DRP.

Fire
Flood
Nuclear power plant emergency
Spilled hazardous materials
Terrorism
Theft
Thunderstorm
Tornado
Winter storm

You as the Security Manager

When working as the security manager, we need to receive the job description for the posting. These guidelines will assist you in determining the extent of your authority. In many organizations, we have an operations manager who is responsible for the building structure, electricity, heat and water. The computer network is inside the building, but we typically do not have to handle room remodeling after a fire, since this would be the operations manager's responsibility.



Now, we will write a job description for the security manager.

Write a Security Manager Job Description

In creating a job description for the security manager, the job title should be at the top, followed by the original date prepared. Next, we put the date revised. The author's name comes next along with the position that they report to.

Title:	Computer Security Supervisor
Date Prepared:	October 24, 2011
Date Revised:	October 24, 2011
Author:	John Smith
Reports to:	Department Manager

Security Manager's General Activates

Next, we need to construct a unique paragraph that describes the general activities of the security manager. These duties should be broad in scope to cover the entire safekeeping of the physical network and the safeguarding of the organization's data.

General Activities:

Over see the inspection of the computer system and facility for any and all security anomalies and report them to the heads of the company. Talk to the supervisor of the previous shift and find out what security issues occurred. Holds daily meetings to discuss the plan for the day with team members. Find and fix any errors employees make while securing the system. Submit reports on security issues on a daily basis.

Write a Security Manager's Responsibilities

The responsibilities of the security manager should reinforce the general activities paragraph. List the responsibilities in order of importance to the organization.

Responsibilities:

- Talk to the supervisor previous shift to find out what security problems occurred the previous shift
- Inspect the system for any anomalies in the security
- Hold regular meetings to discuss the day's plans with team members
- Communicate to heads of the company about current security issues
- Write evaluations on current employees and issue raises
- Find and fix errors of employees
- Coordinate efforts with community security agencies
- Interview and hire new people
- Brief board of directors
- Write annual budget reports

Write a Security Manager's Accuracy and Planning

We expect a high level of accuracy in the security manager's position since this person is probably the third level checker and approver of the network and information. The first level is the computer user, and the second level is the local manager. The security manager should find any errors in the system and correct them immediately.

Accuracy

- 99.999999% accurate

Planning

- Oversee revise and fix all errors in a security code
- Be able to manage time well and lay down a plan for the day
- Submit daily reports on current security issues
- Create and revise a Disaster Recovery Plan (DRP)
- Plan and run DRP exercises on a monthly basis

Write a Security Manager's Communications and Attendance

This level of managing requires better communication skills and almost perfect attendance. In critical position, we need to have a backup and the security manager needs to appoint an assistant to fill in when they are not present.

Communications

- Report to company heads and report on security issues should be made immediately with emphasis on resolving the issue and to avoid repeats of the same problem
- Daily "Security Alerts" will inform the team and managers of threats with definite actions
- Meet with other supervisor to find out about issues
- Write evaluations on employees and suggest raises or employment future
- Brief the board of directors on security matters
- Interview and hire new members for the team

Attendance

- 98% attendance required
- Train an assistant who can supervise during your absence

Assignment

Develop a single page job description for the following personnel:

Security Manager

LAN Manager

LAB Technician

Types of Security

Physical Security –

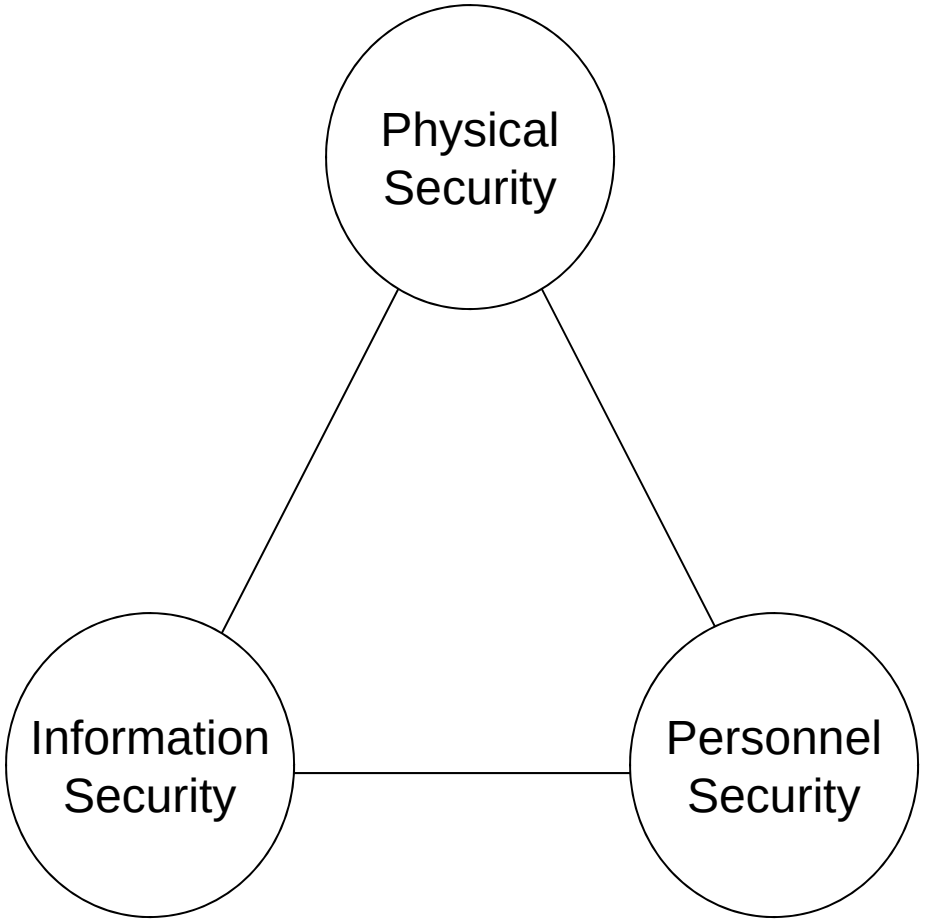
The protection of hardware of any shape and size. This will include operating systems and off the shelf application software.

Information Security –

The safeguarding of the organizations data including custom built applications only available to our organization.

Personnel Security –

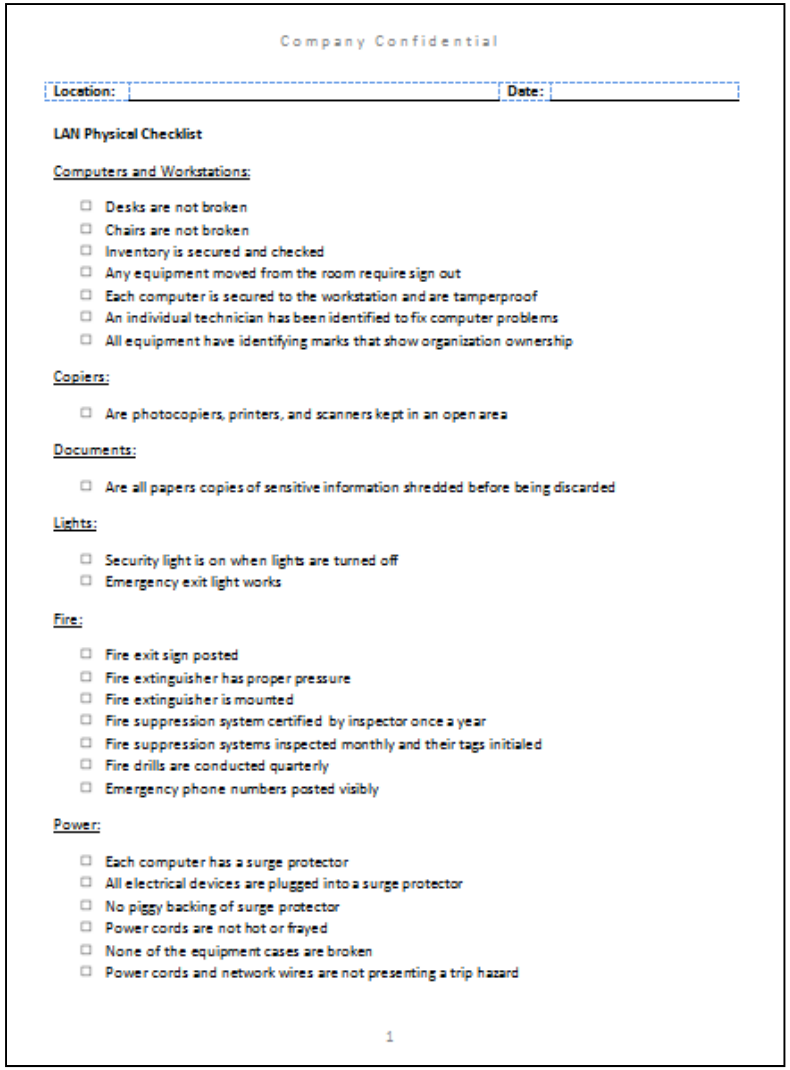
The protection of the human assets of the organization including our customers and partners.



Physical Inspection and Loss

Everyday, a security manager checks the condition of their LAN. Periodically, the team uses a checklist and formally inspects the condition of the entire network. This includes taking inventory and reporting damage.

Simultaneously, representatives of the local government such as fire marshal and building inspector can check the building and rooms to make sure they comply with the law. Companies receiving money from the government or a another institution may have to upgrade their network and facilities to comply with the contract. Failure to accurately report the information can result in loss of payment, fines or both.



Company Confidential

Location: Date:

LAN Physical Checklist

Computers and Workstations:

- ☐ Desks are not broken
- ☐ Chairs are not broken
- ☐ Inventory is secured and checked
- ☐ Any equipment moved from the room require sign out
- ☐ Each computer is secured to the workstation and are tamperproof
- ☐ An individual technician has been identified to fix computer problems
- ☐ All equipment have identifying marks that show organization ownership

Copiers:

- ☐ Are photocopiers, printers, and scanners kept in an open area

Documents:

- ☐ Are all papers copies of sensitive information shredded before being discarded

Lights:

- ☐ Security light is on when lights are turned off
- ☐ Emergency exit light works

Fire:

- ☐ Fire exit sign posted
- ☐ Fire extinguisher has proper pressure
- ☐ Fire extinguisher is mounted
- ☐ Fire suppression system certified by inspector once a year
- ☐ Fire suppression systems inspected monthly and their tags initialed
- ☐ Fire drills are conducted quarterly
- ☐ Emergency phone numbers posted visibly

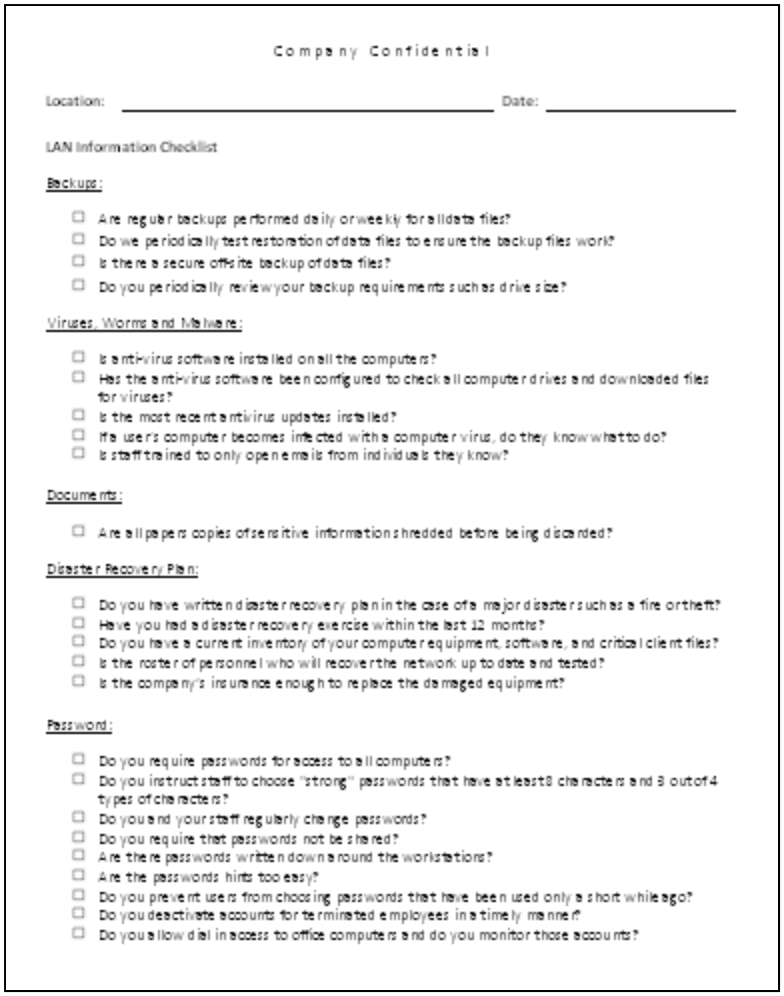
Power:

- ☐ Each computer has a surge protector
- ☐ All electrical devices are plugged into a surge protector
- ☐ No piggy backing of surge protector
- ☐ Power cords are not hot or frayed
- ☐ None of the equipment cases are broken
- ☐ Power cords and network wires are not presenting a trip hazard

1

Information Security Inspection

The data that our organization has is valuable to us and to our competitors. Imagine if you were playing poker and you knew all the cards the other players were holding. We could easily surmise that by the end of the game, the person who knew everybody's information would dominate. Our jobs as security managers is important to the organization since we are the person designated to protect the business' intellectual property which is their number one asset. We do this by only allowing trusted individuals to have access to the data. There are multiple techniques to control access to files to learn as a security manager.



Company Confidential

Location: _____ Date: _____

LAN Information Checklist

Backups:

- ☐ Are regular backups performed daily or weekly for all data files?
- ☐ Do we periodically test restoration of data files to ensure the backup files work?
- ☐ Is there a secure offsite backup of data files?
- ☐ Do you periodically review your backup requirements such as drive size?

Viruses, Worms and Malware:

- ☐ Is antivirus software installed on all the computers?
- ☐ Has the antivirus software been configured to check all computer drives and downloaded files for viruses?
- ☐ Is the most recent antivirus updates installed?
- ☐ If a users computer becomes infected with a computer virus, do they know what to do?
- ☐ Is staff trained to only open e mails from individuals they know?

Documents:

- ☐ Are all papers copies of sensitive information shredded before being discarded?

Disaster Recovery Plan:

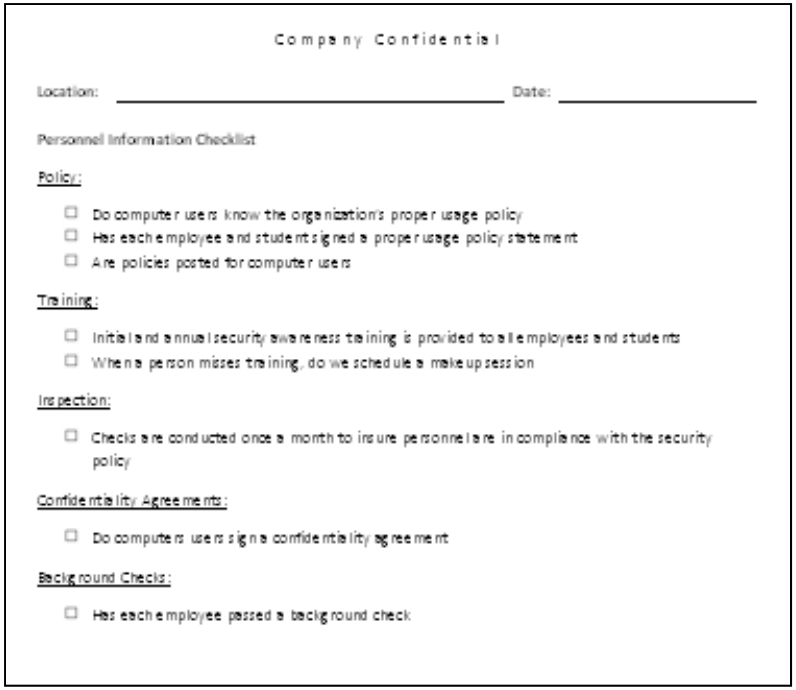
- ☐ Do you have written disaster recovery plan in the case of a major disaster such as a fire or theft?
- ☐ Have you had a disaster recovery exercise within the last 12 months?
- ☐ Do you have a current inventory of your computer equipment, software, and critical client files?
- ☐ Is the roster of personnel who will recover the network up to date and tested?
- ☐ Is the company's insurance enough to replace the damaged equipment?

Password:

- ☐ Do you require passwords for access to all computers?
- ☐ Do you instruct staff to choose "strong" passwords that have at least 8 characters and 3 out of 4 types of characters?
- ☐ Do you and your staff regularly change passwords?
- ☐ Do you require that passwords not be shared?
- ☐ Are there passwords written down around the workstations?
- ☐ Are the passwords hints too easy?
- ☐ Do you prevent users from choosing passwords that have been used only a short while ago?
- ☐ Do you deactivate accounts for terminated employees in a timely manner?
- ☐ Do you allow dial in access to office computers and do you monitor those accounts?

Personnel Security Inspection

A single disgruntled employee can severely damage the reputation of an organization by selling or even giving away sensitive data and equipment. From the United States Pentagon to commercial industries, we have discovered that competitors were given or sold items that were thought to be safe in storage. In our duties as security managers, we need to screen employees, partners and customers to discover the intentions of the people who interact with the network. We need to also protect our employees and customers from those who seek to destroy their contribution.



Company Confidential

Location: _____ Date: _____

Personnel Information Checklist

Policy:

- ☐ Do computer users know the organization's proper usage policy
- ☐ Has each employee and student signed a proper usage policy statement
- ☐ Are policies posted for computer users

Training:

- ☐ Initial and annual security awareness training is provided to all employees and students
- ☐ When a person misses training, do we schedule a make up session

Inspection:

- ☐ Checks are conducted once a month to insure personnel are in compliance with the security policy

Confidentiality Agreements:

- ☐ Do computers users sign a confidentiality agreement

Background Checks:

- ☐ Has each employee passed a background check

Assignment

Develop three security checklists for the organization.

Physical Security Checklist

Information Security Checklist

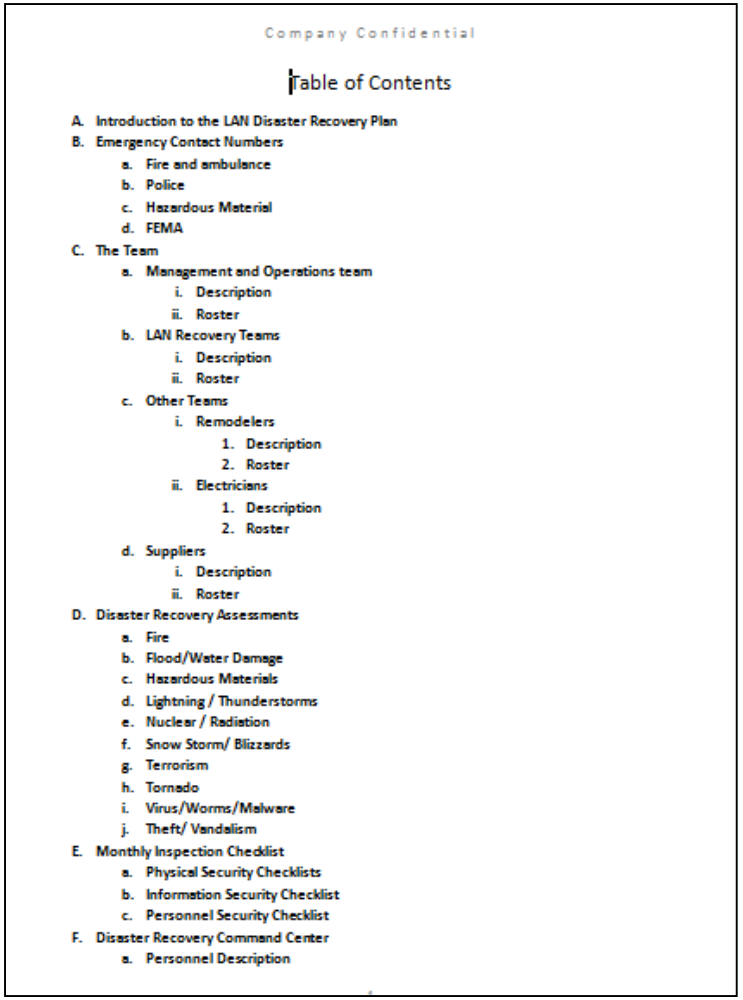
Personnel Security Checklist

Write a Disaster Recovery Plan

A Disaster Recovery Plan (DRP) is a hard bound document that explains every step to recover a full or partial network that has been damaged.

The first DRP we write is the most difficult and over our years of experience, we will become more efficient in developing even larger plans.

Often the first page of the DRP is the emergency contact page and then the table of contents that direct us to specific procedures in the binder. DRP are printed because many times in a tragedy, the electrical systems are inoperable.



Company Confidential

Table of Contents

What is my first DRP?

When choosing your first Disaster Recovery Plan (DRP), we want to start with a commercial LAN where there are a wide range of equipment and that needs to be recovered in a timely manner such as the 48 hour recovery.

Type the following information on the cover page for the DRP with the who, what, where, when, and why data for the organization that you writing the DRP.

Who:	**Smith Mortgages Company John Smith, President**
What:	**Develop a 48 hour recovery plan for their office**
Where:	**1111 Front Street, Columbus, Ohio 43201**
When:	**From October 24, 2011 to December 9, 2011**
Why:	**Company does not have a recovery plan**

DRP Table of Contents

Remember when you were learning a new computer system and you should of written down the step by step procedure. For those who have waited, the DRP contains the exact guidelines to perform every task. These recipes for putting the network back together incase of an attack or disaster fall within a tabbed binder. We want to identify the categories for the DRP

These categories can be emergency contact numbers, DRP team contact information, inventory sheets, command post diagrams and manuals.

What categories do you want for your DRP?

Assignment

Develop a list of categories that would be in DRP
