BUSINESS CONTINUITY/
DISASTER RECOVERY
DigiKnights Technologies

TEAM ONE

NTW440

Disaster Response Plan

Business: DigiKnights Technologies

Date of Current Revision: 7/17/2021

Table of Contents-

Introduction

Address: 2725 E. Technology Ave, Freemont, CA 94536 (The Bay Area)

Scope of Plan: Primary Business – Manufacturing of Computer Game Discs (pressing of the discs) and delivery of those discs to stores nationwide.

Locations where this plan is on file: 2725 E. Technology Ave, Freemont, CA 94536

Authority:

This plan was developed and approved under the authority of:

________________________ ________________________ __________________

Name Title
Date

Immediate Response Phone Tree

- Assess your own safety and act accordingly.
- Elicit help from a co-worker or another person in the area.
- Act to protect lives, then physical property.

Make the following phone calls in the order shown, based on the type of emergency.

1st Priority Calls Type of Emergency	Whom to call
Fire	9-1-1
People Hurt	9-1-1
Water/ Electrical Emergency	9-1-1

2nd Priority Calls Type of Emergency	Whom to call
Building or Equipment Damaged	9-1-1 (Or local maintenance/contractor crew)
Records Damaged	Call IT to retrieve backup.
Computer Equipment Damaged	Call IT

3rd Priority Calls Type of Emergency	Whom to call
All emergencies during working hours	9-1-1
All emergencies after working hours	9-1-1

Identify and create the policy for shelter-in-place procedures including internal assembly points (safe areas), water, water purification tablets, shelf-stable food supplies, clothing, blankets, and other long-term stay materials.

● Close the business. Bring everyone into the room(s). Shut and lock the door(s).

● If there are customers, clients, or visitors in the building, provide for their safety by asking them to stay – not leave. When authorities provide directions to shelter-in-place, they want everyone to take those steps now, where they are, and not drive or walk outdoors.

● Unless there is an imminent threat, ask employees, customers, clients, and visitors to call their emergency contact to let them know where they are and that they are safe.

● Turn on call-forwarding or alternative telephone answering systems or services. If the business has voice mail or an automated attendant, change the recording to indicate that the business is closed, and that staff and visitors remain in the building until authorities advise it is safe to leave.

● Close and lock all windows, exterior doors, and any other openings to the outside.

● If you are told there is danger of explosion, close the window shades, blinds, or curtains.

● Have employees' familiar with your building's mechanical systems turn off all fans, heating, and air conditioning systems. Some systems automatically provide for exchange of inside air with outside air – these systems need to be turned off, sealed, or disabled.

● Gather essential disaster supplies, such as nonperishable food, bottled water, battery-powered radios, first aid supplies, flashlights, batteries, duct tape, plastic sheeting, and plastic garbage bags.

● Select interior room(s) above the ground floor, with the fewest windows or vents. The room(s) should have adequate space for everyone to be able to sit in. Avoid overcrowding by selecting several rooms if necessary. Large storage closets, utility rooms, pantries, copy and conference rooms without exterior windows will work well. Avoid selecting a room with mechanical equipment like ventilation blowers or pipes, because this equipment may not be able to be sealed from the outdoors.

Develop a set of policies and procedures for employees to follow explaining proper safety guidelines.

Training

Proper training needs to be performed beforehand so that everyone is aware of their roles and responsibilities in case of implementation of Business Continuity Plan. 1) Proper Fire Drills need to be carried out quarterly. 2) Network Load should be switched to secondary location with a test run of 2 days once a quarter. 3) Personal safety trainings should be carried out for employees to be aware of what to do in case of disaster 4) Internal auditing needs to be done quarterly to check IT Infrastructure against hacking attempts 5) Trainings should be carried for employees to understand security hygiene 6) Water sprinklers to avoid fires, should be tested once every 6 months

Maintenance This is one of the longest and crucial part of any system or plan. Once everything is implemented, it becomes important to carry out the proper maintenance. It consists of checklists to be created, so that they can be followed in training iterations. Also, Business and its requirements are always dynamic, thus any changes in the business should be checked and same should be implemented in plans while maintenance.

- ● It is ideal to have a hard-wired telephone in the room(s) you select. Call emergency contacts and have the phone available if you need to report a life-threatening condition. Cellular telephone equipment may be overwhelmed or damaged during an emergency.
    - o Use duct tape and plastic sheeting (heavier than food wrap) to seal all cracks around the door(s) and any vents into the room.
  - ● Write down the names of everyone in the room and call your business' designated emergency contact to report who is in the room with you, and their affiliation with your business (employee, visitor, client, customer.)
  - ● Keep listening to the radio or television until you are told all is safe or you are told to evacuate. Local officials may call for evacuation in specific areas at greatest risk in your community.

Goal: Create a checklist for contacting and interviewing a disaster recovery specialist

- Obtain the contact information of a local disaster recovery specialist, ideally one who is experienced with your type of business (physical size, workforce, skillset, etc.)
- Determine the approximate recovery time objective (RTO), amount of time required to recover and resume business operation, and recovery point objective (RPO), the amount of tolerable data loss in time.
- How much did the disaster cut into company profits?
- What is the best way to ensure the customers are aware of the situation?
- What roles and responsibilities should be assigned to the people on the disaster recovery team? How many people should be on the team?

- Ask about an effective communication plan. What is the best way to ensure open lines of communication with the amount of people that are available to get the recovery process moving swiftly?
- Ask about what type of recovery site would be best for your type of business. Make sure to ask about things like location and cost.
- How and how often should the disaster recovery plan be tested and updated.

In-house Emergency Team-

This team will develop, maintain, and implement the emergency management plan,

The team should be made up of employees from all levels, familiar with all functions within the organization. The size of the team will vary, depending on the size of the organization.

Mark Saunders	Senior Management	415-555-8643
Diane Ford	Human Resources	415-555-6312
Linda Kraemer	Corporate Public Relations	415-555-6161
Carlton Bowden	Legal	415-555-3223
Michael Winters	IT Services	415-555-3970
Michael Churchill	Risk Management	415-555-3131
Kenneth Gilliam	Operations	415-555-6431
Katherine Cavenaugh	Purchasing	415-555-3298
Brett Kelcey	Security	415-555-3852

Other Emergency Contacts-

1. Local police department:

Address: 2000 Stevenson Blvd Fremont, CA 94538

Non-Emergency Number: (510) 790-6800

2. Local fire department:

Address: 3300 Capitol Ave. Building A, Fremont CA 94538

Non-Emergency Number: (510) 494-4200

3. Local Hazardous Waste Disposal:

Phone Number: (888) 606-7763

- Local Hospital:

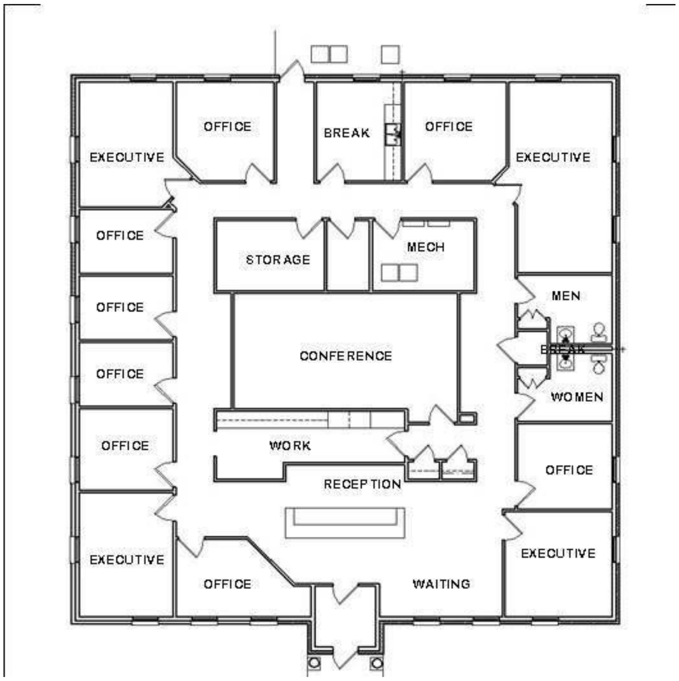
Address: 39400 Paseo Padre Pkwy, Fremont, CA 94538

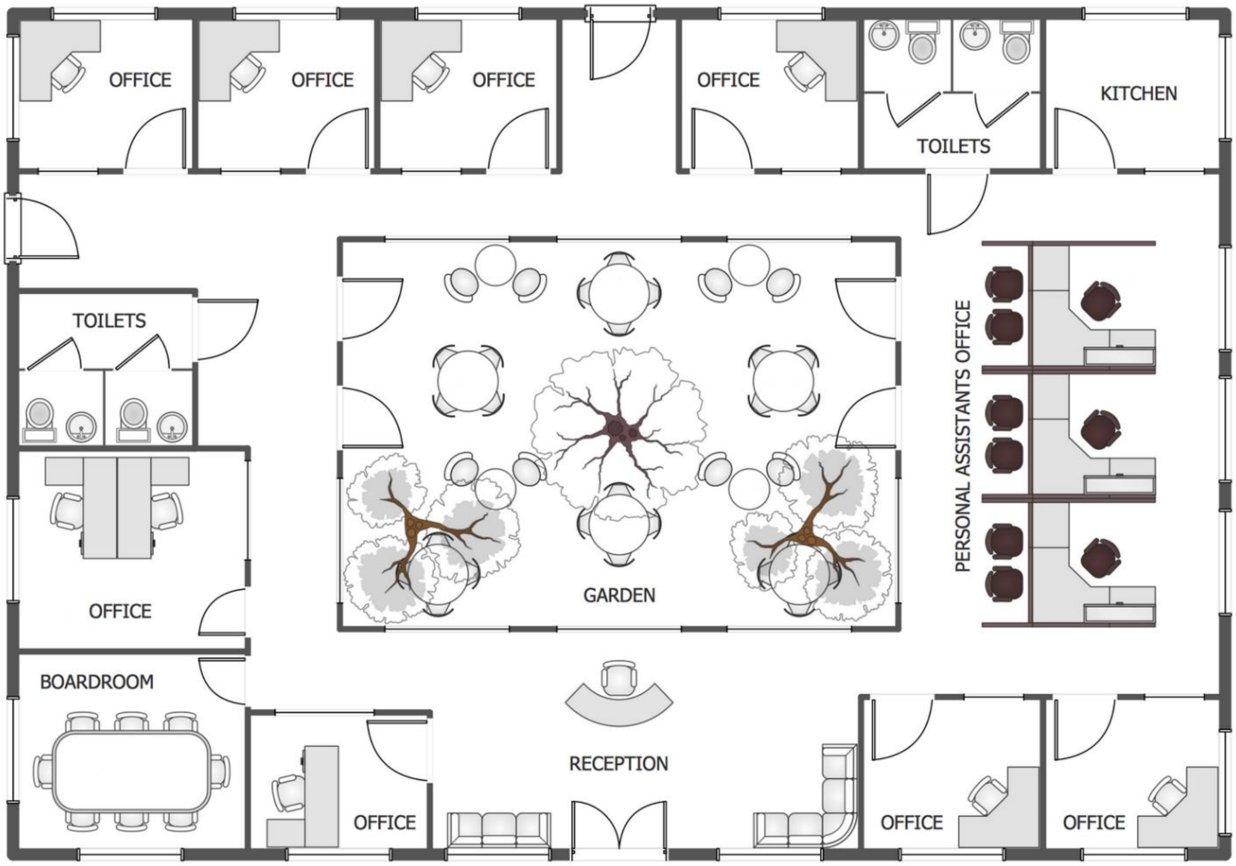
Phone number: (510) 248-3000

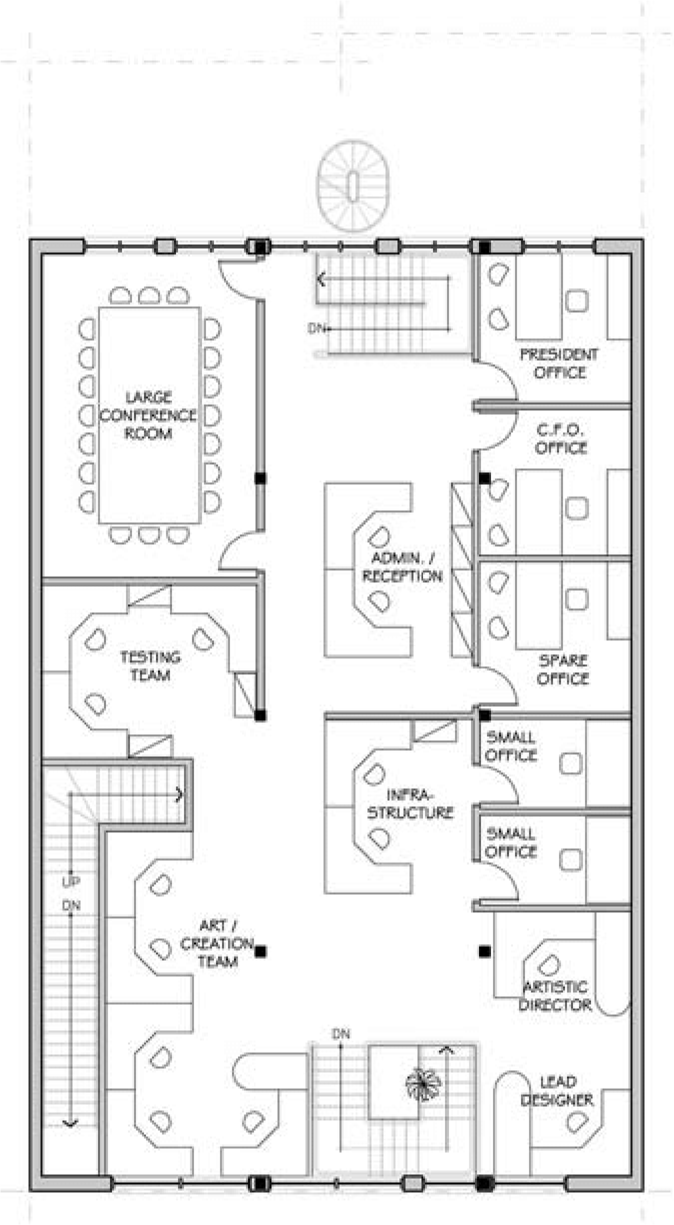
- Emergency: 9-1-1

Facilities: Location of Emergency Systems-

Identify and create the policy for location and testing of alarms, emergency signals, first aid supplies, CPR equipment, fire suppression equipment (fire extinguishers, etc.), and hazardous materials safety equipment--




OFFICE
OFFICE
OFFICE
OFFICE
TOILETS
KITCHEN
TOILETS
GARDEN
PERSONAL ASSISTANTS OFFICE
OFFICE
BOARDROOM
RECEPTION
OFFICE
OFFICE
OFFICE



Location and testing of alarms

Fire alarms should be placed in high traffic locations like major hallways, outside offices, and any location with hazardous chemicals. All fire alarms should be tested every six months by licensed technicians to prevent malfunctions.

Emergency signals

Emergency signals should be placed at every emergency exit of our building. Along with emergency exits, signals should be placed along hallways to light the path to a safe exit. There should also be emergency signals outside of chemical storage to alert to any spills that would cause a disaster.

First aid supplies, CPR equipment

First aid supplies and CPR equipment (AED, and a barrier for mouth to mouth) should be in multiple locations thought the company. For example, in staff break rooms, in the shipping department, the maintenance department, and any other location where there is a risk for injury or chemical exposure. All staff should be fully trained in the use of first aid supplies, AEDs, and Oxygen for use in an emergency.

Fire suppression equipment

The building will be outfitted with fire suppression sprinklers throughout the entire building. There will also be fire extinguishers (types suited for the location they are in) throughout the building, in areas like the break area, the shipping department, the IT room, and placed in key areas to help minimize the damage of a fire.

Hazardous materials safety equipment

At any location that stores chemicals the chemicals will be stored in the proper safety cabinet, one that is fireproof, and made for the chemicals that will be stored in the cabinet. Along with the chemicals being stored in the proper cabinet, there will also be the proper counter ages and containment products to stop a leak and properly dispose of the agent that was leaking.

Goal: Identify and create the policy for evacuation procedures including evacuating, securing, shutting down facility and internal assembly points (safe areas). Be sure to consider the need for local transportation and lodging as well.

Activate the fire alarm and coordinate for someone to call 911

Utilize a fire extinguisher, if necessary, but only if knowledgeable in how to do so

Avoid dangerous areas such as hot doors, or collapsed in parts of the buildings

If smoke is present, stay low and use a cloth (damp preferably) to cover your mouth and nose

Do not under any circumstances use elevators

If capable, assist injured personnel, and if not ensure that medical personnel are notified or someone else who can assist.

Locate the nearest emergency maps, and find the most efficient route out of the building

Assemble all personnel at the designated location from the evacuation map, or wherever the first responders direct you to

Have leaders get a headcount of the people who were assigned to them and ensure that everyone who was in the building is accounted for.

Continue consulting with emergency personnel, providing them with gathered information and gathering information on the state of the situation.

Essential/Vital Business Functions

Prioritize business functions into mission-critical, important, minor.

Definitions:

Mission-critical operations are those processes and functions that are critical to the success of a company. A mission-critical outage is a type of disruption that can have severe financial, legal, and operational repercussions. It is usually considered the most disruptive aspect of a company's operations.

Important operations are the kinds of functions and processes that will not stop the business from operating in the near-term, but they usually have a longer-term impact if they are missing or disabled. From an information technology perspective, these systems are typically used for various business functions, such as e-mail and databases. If they are disabled, these systems can require a moderate amount of time to restore to a fully functional state.

Minor business processes are those that were developed over time to handle small, recurring issues or functions. They should not be lost in the near term while business operations are recovering. From an operational perspective, these types of systems outages can cause minor disruptions to a business. The recovery time typically ranges from weeks to months.

Categories:

- Category 1: Critical functions—Mission-critical (CAT 1)

- Category 2: Necessary functions—Important (CAT2)

- Category 3: Desirable functions—Minor (CAT3)

Prioritize Business Functions into Mission-critical, Important, and Minor.

Shipping Department (CAT1)

Manufacturing/Maintenance (CAT1)

Security (CAT1)

Information Technology (CAT1)

Administration (CAT1)

Sales (CAT2)

Marketing (CAT2)

Research and Development (CAT3)

Departments/Functions

- The **Administration** department
- The **Sales** department manages contacts with stores worldwide, and together with the shipping department ensures the prompt, on-time delivery of products to stores. Utilizing shipping software developed in cooperation with its shipping partners, Digi Knight can accurately track its shipments up to the minute.
- The **Marketing** department is constantly endeavoring to find and maintain publisher contacts, it has proven successful in doing so, and has helped company growth with its findings. research & Development
- The **Research and Development** team; focuses primarily on improvements that can be made to the production system as well as ways to cut manufacturing costs. Its staff maintains contact with other Manufacturing locations to keep up to date with the latest technology.
- The **shipping** department oversees preparing the product for shipment, and in receiving shipments for supplies and materials for producing the physical product.
- The **Manufacturing/Maintenance** department is the workers that maintain the system, and help it prevent non-planned shutdown or machine failure.
- The **Security** department is to maintain the physical security of the facilities and provide a safe work environment for all workers at Digi Knight.
- The **Information Technology** department maintains the technology to support Digi Knight the company, Customers, and Users.

The impact of loss of function for CAT1:

Shipping department: Loss of revenue, higher costs, potential legal liabilities with financial penalties. Loss of customers and suppliers due to companies' problems or may lose customers or suppliers if they experience a business disruption or disaster.

Information Technology: Operational impact the disruption of the IT systems will halt production to all mission critical areas. Legal. Regulations regarding data privacy and security, and other legal constraints. Public relations and credibility.

Security: Legal Regulations regarding worker health and safety and other legal constraints need to be assessed. Staff Retention, loss of product due to theft.

Maintenance/Manufacturing: Operational impact which will lead to a loss of revenue. Legal regulations regarding worker health and safety. Staff retention may be impacted as well.

Admin: Social/Corporate image. Staff retention, finance, and Loss of revenue.

Threat Types:

1. Natural

a. Earthquake

b. Flooding

c. Tornado

d. Hurricane e. Fire

2. Human

a. Corporate Espionage

b. Theft of proprietary information or organizational Intellectual Property

c. Theft of equipment

d. Terrorism

e. Network attack

3. Infrastructure (Physical & network)

a. Faulty construction

b. Power loss

c. Plumbing

d. Device corruption

e. Data loss

f. Disruption of communications

The Impact of various threats to CAT1:

Shipping department: Natural = High **|** Human = Moderate **|** Infrastructure = High

Information Technology: Natural = High **|** Human = High **|** Infrastructure = High

Security: Natural = High **|** Human = Moderate **|** Infrastructure = High

Maintenance/Manufacturing: Natural = High **|** Human = Moderate **|** Infrastructure = High

Admin: Natural = High | Human = Moderate | Infrastructure = High

Maximum tolerable downtime *(*MTD):

• *Category 1*: Mission-critical 12 hours

• *Category 2*: Important— 2 days

• *Category 3*: Minor- 3 days

Recovery time objective (RTO)**:**

Category 1: 4 hours or less

Category 2: 16 hours

Category 3: 1 day

Work recovery time (WRT)**:**

Category 1: 4-8 hours

Category 2: 16-24 hours

Category 3: 1-2 days

Locations of Backup Copies of Essential Records-

Backup copies of all documents, or at minimum essential/vital records, should be stored at another site.

Location – 2725 E. Technology Ave, Freemont, CA 94536

Personnel -

Administration Employees:

Kevin Saunders

Mariam Bell

Jake Huog

IT Employees:

Adam Blue

Sara Davidson

- phone numbers to key personnel including management, BC/DR team, crisis management team, and HR as appropriate.

Cold Site Backup Location Plan

EQUIPMENT-

1. Workstation
2. Printers
3. Network tools and Cables
4. Furniture, such as Desks, Chairs, and more.

RESOURCES ON SITE-

- Internet
- Wi-Fi, Ethernet, or Hotspot connections.
- Power - Provided by the Site Owner
- Heating and Cooling- Provided by the Site Owner
- Restrooms and Water- Provided by the Site Owner

EXECUTIVE SUMMARY-

A Cold Site is a location with basic needs such as power, air conditioning, communication equipment, and more. No equipment is setup on sit, making this the cheapest, but also the longest to set up of the backup locations. This type of location requires that the users are to bring their own equipment in the result of a disaster, which can potentially add costs later on.

High risk of data loses, establishing a concise plan of data transfer from location to location would be a crucial step of the plan regarding this type of site. Calculating how long we have of downtime before problems arise, as well as how long setting up the cold site will take and plan for all circumstances so that the site can be operational in the shortest amount of time. Not having all the equipment already on site leaves the need for equipment to be brought to the cold site, or for new equipment to be purchased. Downtime for this site should be planned to a minimum, as IT will be needed on the project to setup the server, workstations and more to assure for a smooth transition during the incident at hand.

Warm Site Backup Location

EQUIPMENT-

- Server Racks
- Cabling Systems
- Fire protection
- Environment Control

RESOURCES ON SITE-

- Running utilities (Electricity, water, network, etc.)
- Bathrooms
- Office Spaces
- Emergency procedures

Executive Summary

A warm site, by definition, is a backup site which combines the monetary convenience of a cold site, with the ease of setup and operation of a hot site. A warm site is a facility that usually has all the features of an equipped data center, but there is no actual data to be found throughout it. An organization with a relatively short RTO. usually less than a week, that can withstand having their services down for a time like that are the ones who would consider a warm site.

However, since the warm site is a middle ground between hot and cold sites, that means it shares in both their strengths and their weaknesses. The strengths of a warm site are in its efficiency to be up and running and similar server power as the main site. The warm site has most of the necessary equipment to function right off the bat, meaning there only need to be minor things brought in, of course along with all the data. It also is usually similar in server power, which includes things like size and storage. The main downside of a warm site is the cost of maintaining it. Since a company is not going to use the warm site, ideally, then it does become an extra insurance-like cost. The warm site cost less than a hot site, which must be fully backed up and operational, and more than a cold site, which is effectively just rented space. A warm sites usefulness will depend mainly on how much the company is willing to spend, and if their RTO aligns with something within the restrictions of the warm site.

Hot Site:

Equipment:1-Electricity2-Servers3-Conferenceroom4-Waterservices5-Wasteservices6-Exercisearea7-Areas to change clothes if needed

Execute Summary: For hot sites, it essentially a replica of the main site. Almost all the equipment is the same with both sites, the biggest difference is the location. The hot site would want to be far away from the main site, like in a different state or across the country because if something goes wrong near the main site, the hot site needs to be able to immediately switch over. The hot site essentially will always be running and online in case the primary site has something go wrong like a power outage or an earthquake, the hot site can immediately take over. Out of all the backup sites, the hot one is the most expensive because it needs to have all the necessary equipment ready to be used immediately. The hot sit will also take the longest to set up because it will need to have the same equipment that the main site has and that can take a long time to set up. The pros to having a hot site is that it is immediately ready to be switched over from the primary site. The cons to having a hot site is that it is very expensive to maintain because all the equipment and employees need to be ready to start working like they would at the primary site which could cost a lot of money. It will essentially cost the same amount that the primary site will cost.

Mobile Site Backup

EQUIPMENT-

- Server Rack.
- ESXi Server, cloned to a recent backup copy of our data.
- Full set of Networking gear.
- 50 workstations for employees
- Airconditioned tents for employees to work in
- A large airconditioned trailer to hold all the gear when not in use, and for the IT team to work in while the trailer is deployed.
- Printers
- Disk Burners
- Fiber cables
- Ethernet cables

RESOURCES-

1. Internet, satellite, or LTE or both for a backup
2. Generators
3. Fuel
4. Porta potty
5. Water source

Executive Summary:

A mobile site is a quick and easy way to quickly deploy a backup site when a disaster hits our main site. With this mobile site we can setup are operation anywhere; this can be helpful if our other backup sites are a no go, due to weather or any other reason. It can also be helpful if we get setup and must quickly move sites due to a bad storm.

The mobile site is very quick to get setup, provided the operations trailer has been setup properly before any disaster hits. When we need to deploy our mobile site, all that should need to be setup is a large tent for all the employees to work under, this tent should be air conditioned, so it is safe and comfortable to work in no matter the outside weather conditions.

There is a small downside to a mobile site, it is mobile which means if it is not guarded around the clock, it could be stolen with the server rack inside. It is also all outside which means it is more exposed to the elements then a normal building which could mean the tent and the equipment inside the tent could get damaged with the weather takes a turn for the worse.

Definitions: A mirrored site is a fully redundant web server/site that mirrors the events happening in the live site. This method of risk mitigation provides the highest degree of availability, and it also allows the server to process all transactions simultaneously. Equipment Needed Totals Switches Computers Printers 10 60 15Ten (10) Servers• PowerEdge R620•16 GB of RAM•3 X 2 TB Hard Drive (configured to RAID 5) • Windows Server 2016•Dual Gigabit Network Cards•15 Inch Monitor Five (5) Workstations • Intel Quad Core i7-4470•16 GB of RAM•1 TB SSD Hard Drive • Built-In Video Card • Gigabit Network Card•21 Inch Monitor • Windows 10.

Equipment/Resources

•Electricity

•Ethernet Cables

•Servers

•Computers

•Workstations

•Conference room

•Restrooms

•Water services

•Waste services

Mirror Backup/Site A mirror backup, or a full image backup, is a copy of the source data set, but only the latest version of the data is stored; not tracking any changes. All individual backup files are stored separately, the same as in the source data, rather than in compressed backup files like the other methods. This allows for quick access to individual files instead of restoring the whole data set, which can be useful. If, a computer malfunctions and disaster recovery must be initiated, mirrored solutions work through a hot swap system or a hot stand by disk system to save data. In a hot swap system, the system itself signals a disk failure and switches over to the mirrored disk. Users frequently do not even know that this was done, except for an alert that may pop up on their screen. The pros of a mirrored site are fast data recovery, and access to individual files/folders. Cons are its very expensive, large storage requirements, and when files are deleted, they are also deleted from the mirror; meaning adverse modifications to the source data could also impact the mirror backup regarding the data.

VMWare Backup

What data is backed up.

When it comes to backing up VMWare infrastructure there are two important things to back up, the virtual machines that are deployed on the server and the server configuration files. The hardest part of this is backing up the VM’s themselves, luckily there is a nice tool to make backing up VM’s easy. That tool is called Veeam; with Veeam we can fully backup our virtual machines safely and quickly.

For our ESXi configuration files we will need to use the ESXi host's command line to create a simple script that will back up all our ESXi host config files. To make are life easier we would want to save the backup file on a network share so we can have a backup outside the host server.

Where is the data backed up to?

I am a big supporter of the free and open-source community, that is why my recommendation is that all our data is backup to a TrueNAS server on our network. We would also use a service called Tarsnap to have a cloud source to keep our data backed up offsite as well. I am also a firm believer of the 3-2-1, which means we have a total of 3 copies of the data, the primary copy and two backups. Plus, the data is stored on two types of media, for our backups that would be our TrueNAS file server, and a Tap drive that is updated at least once a month. Lastly, we keep one copy in the cloud.

What software is used for the backup.

We would be using a mix of software for our backups. First, we would use Veeam to create the backup files that would be stored on our TrueNAS server. Once that copy has been created, Tarsnap would be used to send a copy of our backed-up data to a secure cloud storage location. Lastly, we would also use the software required for a tape drive once a month to keep a second copy of our data offsite, secure in a safe deposit box.

Would the backup be incremental or full or both?

Our backups would be a mix of incremental and full. The type of backup that would be run the most would be an incremental, and that would run nightly; however, once a month we would run a full backup to keep a good mix of data and system configurations.

How long would the backups take based on the method of replication?

This can be a bit of a hard question to answer since we will be using multiple types of backup methods. However, the first full image would most likely take a weekend to complete. It would also most likely take a weekend for each full back up as we would need to back up every system on the ESXi host. The nightly incremental backups would be able to complete each night.

For our push to the cloud, that would also take a weekend to complete the first initial push with all our data, however like the incremental backups all our subsequent backups would be pushed to the cloud relatively quickly because of the way Tarsnap works to help save space and money when backing up with their service.

What is a good method of backing up the vCSA appliance?

A good method of backing up the vCSA is with Veeam also. We would want to create a two-part backup process, first we would use Veeam to create an image level backup then we would use VMWare best practice to make a backup of the database since unfortunately Veeam does not support Postgres SQL, the DB of ESXi, and push that database backup to our cloud and tape backup copies.

Vendor Lists

Below is a List of all the DigiKnight Vendors, to act as a backup vendor list so that backup equipment can be purchased in the event of an emergency to keep the company running.

Computer Vendors

Dell – Computer Systems

Call – 1-800-WWW-DELL

Address – One Dell Way, Round Rock Texas 78682

Contract Number – 42368131588-DGK

HP – Computer Systems

Call – 800-282-6672

Address – 3000 Hanover Street, Palo Alto CA 94304-1185

Contract Number – DGK-13548253

Bold Data Technology, Inc. – Maintenance Personnel

Call – 800-923-2653

Address – 48363 Fremont Blvd. Fremont CA 94538

Contract Number – DGK1161

Risk Assessment-

Natural Threats

5 Major Natural Threats to the company

- **Earthquakes**
- **Flooding**
- **Fires/Wildfires**
- **Tornado**
- **Volcano**

It is expected of us to find how these threats can affect us, what we can do in a situation involving these threats, and what the downtime looks like when one of these threats occurs. All research is done regarding the location of the DigiKnights Company Buildings based in Fremont California. These risks are rated from a scale of LOW, MEDUIM, and HIGH risk to the company, its suppliers, and any other associated parties.

Earthquakes- HIGH RISK

Fremont resides along a major fault line, making the area and its inhabitants prone to the threat of earthquakes. According to a study, there is a 63 percent chance in the next 30 years for The Bay Area to experience a magnitude 6.7 or higher earthquake, affecting over two million people. An earthquake that we know has the potential to happen, but not the know of when, is an obstacle we must overcome. In preparation, well as planning strategies to protect our company, employees, products, suppliers and more.

Here are some of the earthquake related threats we have identified in our research-

- Evacuations from earthquakes in the area could halt progress on ongoing projects and due dates. This would also halt/slow the transportation to and from suppliers during the earthquake, as the usual route to the buildings may be changed or nonexistent from the potential damage the earthquake could cause.
- Internet connection may become spotty or stop because of the damage to local towers, as well as Power being out, resulting in downtime.
- Damage to the buildings, and their holdings are a potential threat in the chance of an earthquake. Construction to the buildings, as well as replacing damaged goods or resources in the buildings, would need to take place.

- While the evacuations may slow down progress of transported supplies to the buildings, so could the event of an earthquake as well. Whether our location or the location of other supplies become damaged because of the earthquake, this could halt the shipping of necessary resources to the company that could affect our schedules and the like.

Flooding- MEDUIM RISK

Sea levels are on a slow but constant rise due to climate change. This constant rise could lead to an increase in flooding and other such water-related events, which could be a problem in the future for this company. Studies show a rise in coastal flooding in the Bay Area over the years with climate linked sea levels rising. Graphs show that even with a slowly increasing sea level, there is a 76 percent chance of a three foot or higher flood happening between 2021 and 2050 in the Fremont area. Regarding the now, there is just under 20 percent of all houses in the Fremont area at risk for flooding, totaling around 11k properties at risk. These numbers only rise as we can see when looking at data collected over the years.

Here are some of the flood related threats we have identified in our research-

- Flooding could result in company property (Building, Vehicles, etc.) as well as supplier equipment being damaged, or just not allowed to access the area. This damage could halt current projects in the company to adjust for the new damages, as well as new routes and dates made for suppliers and drivers.
- Flooding will damage public utilities, as well as internet and power resources in the area, resulting in a potential undetermined amount of downtime on these resources.
- Clean-up will become part of the plan to come back to the buildings once the OKAY is given by public authorities. Employees may be designated to help with the cleanup, should the position be entitled so.
- Like Earthquakes evacuations, Flooding will halt progress across the company. There could be days or weeks of downtime depending on the severity of the flood, and how long the cleanup may take.

Fire/Wildfire- LOW RISK

Fremont is right outside some of California's Elevated and Extreme Fire Prone Areas, according to a Map provided by ABC. This means, while we are not in the area to begin with, does not mean we should plan for the occurrence of the fire spreading to our area. Wildfires seem to be a constant threat to the state of California, and the state thankfully has saved a lot of people's lives by providing quick and adequate responses to the people and businesses who reside in the way of damage.

Here are some of the fire related threats we have identified in our research-

- Fire hitting electrical lines or equipment could be very dangerous and could result in power being unavailable for days or weeks. Alternate power options could be available, should the downtime of the electricity be too great.
- Damage caused to the outside of company buildings, property or resources could affect the dates of in progress maintenance work on the building and could result in alternate housing for employees and company equipment should the damage mean long repair times.
- Supplier deliveries expected project due dates, and any other scheduled events would need to be halted to deal with the situation. Rescheduling and other needed updates will be created when the time allows after the situation has been contained.

Tornado- LOW RISK

The risk of a tornado in Fremont is significantly lower than the national average. There have only been two recorded historical tornado events in the area, the latter being around 1951, and the most recent being 1998. These recorded tornados have a two rating out of five. California only experiences around 6-7 total tornados a year, with 94 percent of them being a one or lower rated on the Enhanced Fujita Scale

Here are some of the tornado related threats we have identified in our research-

1. Like most events, planning is the key to protecting our most valuable resources. If given notice about the earthquakes, we could find ways to best secure our buildings, as well as our products, resources, and employees are safe from the damage.
2. Strong winds and debris could damage or destroy company property, as well as affect power, water, and other vital resources to the company. After assessing the damage from the tornado, new project dates, scheduled deliveries and more can be reassigned and work can go back to normal after a few days or weeks of potential downtime.

Volcano- LOW RISK

The start of the paragraph- The lowest risk of the natural threats, volcanoes have a very small chance of making landfall in the bay area. Should one of these volcanoes become a threat, the DRP will be updated. While California may have 15 known volcanoes, the closest to the company would be over 150 miles away north, known as Clear Lake Volcanic Fields.

Here are some of the volcano related threats we have identified in our research-

- Follow any evacuations that may be issued by state or local authorities. These will be very new to everyone, and will most definitely halt company projects, deliveries, and the like.
- In the event of a phenomenon called Ashfall, people are instructed to stay indoors at all costs, and to only go outside with the assistance of a respirator. Lastly, sealing all open-air vents, doors, and windows
- Being a new event in the area, should a threat like this arise, downtime is expected. Current projects, scheduled deliveries, and other associated tasks will be put aside while dealing with the threat.

Conclusion

All these events would be intense planning, strategy, and complete cooperation from all company employees. Evacuations could be necessary for all these incidents, as well as a need for new plans to be adjusted constantly in the wake of an event such as these. Disaster Kits and careful training for these types of events will be crucial to company resources and employees to become familiar with.

Man-made Threats

Man-made threats are the more common threats to businesses and their networks and data. These can come in the form of a direct attack on a system in the form of hackers, spam, viruses, and worms. They can also show themselves in the form of credit card fraud and identity theft from data stolen from companies' systems. Also, terrorism is a constant threat to businesses.

A non-physical threat is a potential cause of an incident that may result in.

- Loss or corruption of system data
- Disrupt business operations that rely on computer systems.
- Loss of sensitive information
- Illegal monitoring of activities on computer systems
- Cyber Security Breaches
- Others

The non-physical threats are also known as logical threats. The following list is the common types of non-physical threats.

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

To protect computer systems from the above-mentioned threats, an organization must have logical security measures in place. To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software. In addition to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visit the website that is most likely to download unauthorized programs onto the user's computer.

Unauthorized access to computer system resources can be prevented using authentication methods. The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.

Intrusion-detection/prevention systems can be used to protect against denial-of-service attacks. There are other measures too that can be put in place to avoid denial of service attacks.

More than 34% of businesses around the globe are affected by insider threats yearly. 66% of organizations consider malicious insider attacks or accidental breaches more likely than external attacks. Over the last two years, the number of insider incidents has increased by 47%.

Computer security vulnerabilities can be divided into numerous types based on different criteria such as where the vulnerability exists, what caused it, or how it could be used. Human Vulnerabilities. The weakest link in many cybersecurity architectures is the human element. User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.

Hidden Backdoor Programs

This is an example of an intentionally created computer security vulnerability. When a manufacturer of computer components, software, or whole computers installs a program or bit of code designed to allow a computer to be remotely accessed (typically for diagnostic, configuration, or technical support purposes), that access program is called a backdoor.

When the backdoor is installed into computers without the user's knowledge, it can be called a hidden backdoor program. Hidden backdoors are an enormous software vulnerability because they make it all too easy for someone with knowledge of the backdoor to illicitly access the affected computer system and any network it is connected to.

Because information security risk is the likelihood of monetary loss, no matter which approach you choose, the first step is to think about how your organization makes money, how employees and assets affect the profitability of the business, and what risks could result in large monetary losses for the company. After that, you should think about how you could enhance your IT infrastructure to reduce the risks that could lead to the largest financial losses.

Attackers can alter electronic data or steal and misuse it or gain unlawful use of a computer or system. For example, if someone successfully uses fraudulent data to purchase a product from your online store, your company will lose money. Therefore, you need to implement a process or solution that will prevent fraud, or at least mitigate the risk of fraud.

IT and technology-based threats

5 Major IT and Technology Based Threats

- Malicious Software
- Corrupted Data
- Software Bugs
- Outdated Software
- Neglecting Proper Configuration

Malicious Software - Low Risk

When it comes to IT and other technology-based threats, malicious software is some of the first things that people think of, and for good reason too. However, in the world of servers and data centers it seems like this is somewhat of an unjustified fear. When you start going into the statistics of the downtime caused to servers, the main threat for servers is actual human error. Malicious software does not even make it into the top 5 when discussing the threats to a server's uptime. However, this does not mean that malware is a nonexistent threat and should be taken lightly.

Here are some of the Malicious Software and Virus threats

- Malicious software is somewhat of a broad term and encompasses all forms of programs that could be possibly harmful to a server or data center. Malicious software can be put into smaller subcategories such as viruses, worms, trojan horse, etc.
- The main purpose of malicious software when it is attacking a system is to steal, modify, or delete sensitive information from a database in a way that is advantageous to the attacking party, or even an organization that went about employing the attacking group.

Corrupted Data - Low Risk

Data corruption is usually that effect of some other event, however it does come with its own host of problems that can affect the server in a negative way. Corrupted data does not commonly put a server down, but it can cause problems on the smaller parts within the server and may cause some smaller malfunctions. Overall, corrupted data is not an extremely high-risk threat and if taken care of swiftly won't cause problems on too large of a scale.

- Data corruption usually happens due to some form or hardware failure, whether that be on the power, network, or actual server hardware that causes it. Power and network outages are not particularly easy to predict or prevent, since that area lies out of the control of the company. The other cause of data corruption is failure of the server-side components, including the hard disks and problems that form over time due to neglected, unmanaged large databases.

- Corrupted data is a fairly common problem, but it can also be an easy one to prevent and recover from. There are many ways to put this into action, and these are some of the most common ones. Firstly, maintaining regular backups to ensure that corrupted data can be replaced and there is not a huge loss. Next, splitting up the databases to avoid one huge conglomerate that can become unmanageable and corrupted. Finally, hardware maintenance and repair to keep server equipment functional and efficient.

Software Bugs - Medium Risk

Software bugs are another common thing that people in the field understand and expect, but people outside of the field rarely seem to mention. Software bugs can be very small, and pose maybe a slight inconvenience at best, or very large, and especially if involved in security can become difficult problems to deal with.

- Software bugs are prevalent in all types of computing devices, simply because coding is such a specific task, and attempting to account for every single variable and having it run perfectly is not feasible. Even the smallest of failures in having the code understand or perform a certain way could cause a bug in the software.
- Software bugs depend usually on the creator, or team that created it to rectify the problems. Because of this, most problems will be out of your control, which could be catastrophic in the event of a security related bug, or anything similar. To try and prevent these bugs from popping up ensure the software used fits the use case, and any software that is being used is up to date with the latest version that has been pushed out.

Outdated Software - Medium Risk

Using outdated software seems like a bad idea all around, but there are certain use cases which make it seem like a more enticing option. For example, the newer software being more expensive and thus using the older one to save on costs. However, using outdated software can come with some large risks, especially if it is one of the more integral pieces within the system.

- Some of the previously referenced integral pieces of software that may cause large scale problems if they are outdated include things like DCIM software for data centers. At best, the bugs might just be small visual glitches, but at worst they could be glaring security flaws that may be exploited by attackers.
- Outdated software can also cause conflicts with other programs and may make the actual process of managing everything much more complex that it needs to be.
- Fixing outdated software is as simple as either updating the version that you have or paying for the update or latest version from whoever the distributor is.

Neglecting Proper Installation - High Risk

Neglecting proper installation does not necessarily only happen at the beginning of the life of a server or data center, but also includes when there are upgrades or remodels that take place. Improperly installing the server racks, network switches, or any other gear that the servers may utilize could come back to haunt you in the future.

- There are two main reasons that would cause one to neglect proper installation of new hardware or software. The first is financial, since it can be expensive to get the right skill set required for the installation. The other cause is time. New installations might take a while, and especially if it causes a portion of the server to go down it could cut into profits.
- The only fix to neglecting proper installation is to ensure that the new hardware or software is being properly installed. This is easily justified by the amount of hassle it may save in the future, due to improper installations starting to cause problems that usually require an overhaul of the original installation anyway.

Above were five IT and technology-based threats that could be a possible danger to the health and efficiency of the server center. The good thing about these threats is that they are mostly all solved just with a little bit of foresight. Ensuring that your software is up to date and working properly, ensuring data is correctly backed up to account for corrupted or lost data, not properly installing new or replacing old parts, and ensuring that security is not neglected for the threat of malicious programs. All these things can be done before, and completely or for the most part diminish the effect that would occur based on the threat.

Environmental/infrastructure threats

Threat Types:

Natural-

Earthquake

Flooding

Tornado

Hurricane

Fire

Human-

Corporate Espionage

Theft of proprietary information or organizational Intellectual Property

Theft of equipment

Terrorism

Network attack

Infrastructure (Physical & network)

Faulty construction

Power loss

Plumbing

Device corruption

Data loss

Disruption of communications

Threat Matrix:

Threat Name	Threat Source	Risk	Frequency	Controls	Impact	Residual Risk
Earthquake	External	High	Rare	Structural Engineered	High	Low
Flooding	External	Low	Infrequent	Pumps, Drainage	Low	Very Low
Tornado	External	Low	Rare	None	Low	Very Low
Hurricane	External	Low	Seasonal	Reinforced Windows	Mediu m	Very Low
Fire	Both	Low	Rare	Sprinklers, Fire Extinguishers		Low
Corporate Espionage	Both	High	Rare	Security, Network Security	Very High	Low
Theft of Proprietary Information	Both	Medium	Infrequent	Security	High	Low
Theft of Equipment	Internal	Low	Occasionally	Security	High	Low
Terrorism	External	Low	Never	Security	High	Low
Network Attack	Both	High	Frequent	Network Security Implementation	High	Low
Faulty Construction	Internal	High	Rare	N/A	High	Medium
Power Loss	External	High	Infrequent	N/A	Mediu m	Low

Plumbing	Both	Low	Very Infrequent	N/A	Medium	Low
Device Corruption	Both	Medium	Frequent	N/A	Very High	Low
Data Loss	Internal	High	Infrequent	N/A	Very High	Low

Frequency:

Rare – Annual or longer

Seasonal – A range of months annually that the threat occurs.

Infrequent – Occurs every 6-12 months.

Occasionally – Occurs every 1-30 days.

Frequent – Occurs every 1-6 months.

Never – Never happens but remains a threat.

Risks:

Very Low – May impact business activities but will cause no outages.

Low – May cause minor outages.

Medium – Will cause outages and cost the company business.

High–Business will cease until problems are fixed.

Very High – Business may lose customers or shut down completely if threat is not fixed in a timely manner.

The threats were ranked based on the likelihood of the event taken place and their vulnerability.

List of the percentage of upstream and downstream loss during the event

Natural Threats:

Earthquake-

upstream: 45%

Downstream: 45%

Wildfire-

Upstream: 75%

Downstream: 75%

Tornado-

Upstream: 55%

Downstream: 55%

Hurricane-

Upstream: 100%

Downstream: 100%

Earthquake-

Upstream: 45%

Downstream: 45%

Man-made Threats

Competition-

Upstream: 50%

Downstream: 50%

Malicious Individual (Hacktivists, hacker group, etc…)-

Upstream: 50%

Downstream: 50%

Disgruntled Employees-

Upstream: 10%

Downstream: 25%

Politically Motivated Individuals-

Upstream: 50%

Downstream: 50%

Corporate Espionage-

Upstream: 30%

Downstream: 25%

IT and Technology-based Threats

Severe Weather-

Upstream: 75%

Downstream: 75%

Malicious Software-

Upstream: 100%

Downstream: 100%

Corrupted Data-

Upstream: 50%

Downstream: 50%

Software Bugs-

Upstream: 50%

Downstream: 50%

Virus-

Upstream: 40%

Downstream: 45%

Environmental/Infrastructure Threats

Wildfire-

Upstream: 75%

Downstream: 75%

Earthquakes-

Upstream: 45%

Downstream: 45%

Flash Flood-

Upstream: 25%

Downstream: 25%

Tornado-

Upstream: 10%

Downstream: 10%

Hurricane-

Upstream: 5%

Downstream: 5%

Create an assessment for determining inventory or list of critical resources at damaged site.

This assessment will have three different ratings for 3 different levels of situations to help accurately gauge the issue, and what needs to be done to resolve it. The first level, level 1, is the lowest damaging rating. When assessed a one, there are mainly minor with some medium difficulty fixes, and is light on the budget. A level 2 rating will be given in a situation in which the financial strain and problems are anywhere from low too high in cost and difficulty but can be averaged out to around medium. Finally, a level 3 rating will indicate that there is severe damage. The financial burden and difficulty for a level 3 assessment are remarkably high on the company and could lead to problems beyond the original such as downtime and finances. This assessment system provides a scale to help a business or company better prepare for a situation based of an initial canvassing.

Level One:

An example of a level one rating will be things such as power or network outages. These identify as a level one for several reasons. First, the economic responsibility is small, as the power or network outages are out of their control, the business just needs to focus on possible data corruption or data loss. Two, especially if a business is up to date on backups there would be little to no cost to them besides the downtime. There would be no cost for restoration for the company unless the issue was completely neglected. However, if the issue is neglected some costs, such as overheating/overcooling of equipment might come into play depending on location, since the room may no longer be a controlled environment.

Level 2:

An example of a level two rating would be anything that could cause an extended downtime and a medium high financial burden. Things that would be in this section could be flooding and tornadoes. These situations are likely to cause a lot of small damage, or one cluster of a lot of damage. The financial burden and downtime would correlate to how fast the situation is to get under control. Assuming something like a flood, the longer the components are under or near water the longer they must become damaged and unsalvageable. In this scenario, approximately half of the damaged resources may be able to have their data recovered, but most of the physical hardware would be destroyed.

Level 3:

A level three rating is the worst assessment and indicates major damage to the infrastructure and/or data loss. Examples of something that may cause this rating would be hurricanes and earthquakes, as they can be absolutely devastating. With a level 3 rating, the company will experience long amounts of downtime on that main site, almost forcing them to initiate a backup. Most of the equipment and data will be unrecoverable, and the financial loss would be devastating. A level three disaster could raze a company in one fell swoop if said company has not prepared for the disaster.

Inspect for hazardous materials, chemicals, or hazardous conditions.

DEFINITIONS:

Hazardous Material: A product, waste, or combination of substances which because of its quantity, concentration, physical, chemical, toxic, radioactive, or infectious characteristics may reasonably pose a significant, actual, or potential hazard to human health, safety, welfare, or the environment when improperly treated, stored, transported, used, disposed of, or otherwise managed. Hazardous materials include - without limitation - synthetic organic chemicals, petroleum products, heavy metals, radioactive or infectious materials, and all substances defines as "toxic" or "hazardous" under California Law.

Handling and use of Hazardous Material:

Storage

- All hazardous material must be stored in appropriate cabinets, flammable material storage cabinets etc. until use and returned for safekeeping after use. Containers of hazardous materials should not be left on bench tops when not in use.

MSDS Information

- It is important that anyone using hazardous material read the Safety Data Sheet (SDS) associated with the hazardous material before its use.
- Anyone handling or using hazardous material shall use personal protective equipment as noted in the SDS or as indicated in the Amherst College Chemical Hygiene Plan.

Disposal of empty hazardous material containers

- If the entire contents of a hazardous material container are consumed, the empty container shall be wanted to read the bar code to decrement the quantity in the CIS.
- Empty containers may be discarded into a "Glass Only" box or a wastebasket as appropriate. A container is considered empty if the contents have been removed by the normal procedure for that hazardous material, pouring, scooping, etc.

Hazardous material on-hand without use

- Any hazardous material which is deemed unacceptable for future use or is identified as excess material without future need, will be declared hazardous waste by attachment of the appropriate hazardous waste label and managed in accordance with the Amherst College Hazardous Waste Management Policy.

In the event of a chemical spill, follow the instructions on the procedure below:

Evacuate the spill area. Aid including the use of safety showers and eyewashes. Seek emergency medical assistance once properly decontaminated.

Confine the spill area by closing the nearest doors to the spill area. Isolate contaminated persons and do not allow them to leave or spread the contamination. Cover drains to prevent spills from entering the environment.

Immediately report the spill to the appropriate emergency response office as specified below in the material specific spill cleanup procedures. Provide information on injured staff, type of hazardous material spilled, estimated quantity, and location. NYP Security can be contacted during off-hours to report hazardous materials spills.

Secure the area until emergency response personnel arrive to ensure no one enters the spill area. If the area has multiple entrances, be sure to locate staff at all entrances to prevent entry.

Cleanup must only be conducted by qualified personnel with the appropriate training, protective equipment, and cleanup materials. Depending on the nature and size of the spill, trained department or laboratory staff may be able to clean up the spill as specified below. Otherwise, emergency response staff are available 24-hours / 7-days a week to respond.

DEFINITIONS:

Hazardous Conditions - Any set of circumstances, which significantly increases the likelihood of a serious physical outcome. A Hazardous Condition reporting form will be utilized by any employee to report a possible hazardous condition (see attachment). Examples of hazardous conditions that should be reported include, but are not limited to, malfunctioning doors, broken equipment, burned out lights, uneven surfaces along walkways, etc.

PROCEDURE:

All employees are responsible for identifying potentially hazardous condition and taking immediate action to ensure the safety of others.

The staff member will then immediately notify their immediate supervisor of the potentially hazardous condition.

The supervisor will evaluate the situation and if necessary, take any necessary immediate action to mitigate the hazard. A Hazardous Condition Reporting Form will be completed by the supervisor and forwarded to the Safety Officer.

The form will be forwarded to the Safety Officer within 24 hours. The Supervisor will also submit a work order to the Maintenance Department if necessary. A copy of the work order must be attached to the Hazardous Conditions Reporting Form which is forwarded to the Safety Officer.

The Safety Officer will evaluate the reported hazard and report back to the originating employee and the Supervisor with the findings of the evaluation. The Supervisor will review each Hazardous Reporting Form and determine whether further action is necessary.

For those issues that are in fact hazardous but cannot be remedied i.e., train tracks, fishing pond etc., reasonable action will be taken to mitigate the potential for risk.

Inspect resources and vital records for damage including water, fire, water, dust, ice, or physical damage (crushed, tipped over, etc.)

In the event of a flood or broken water pipe within the facilities, follow the instruction on the procedure below:

- See if the emergency can be contained by turning off the water main, or nearest source of water. If it is flooding, try to contain the flooding to one area and try to plug the source.
- Notify maintenance immediately to shut down power to the affected area of the building to help prevent any electrical fires that may trigger from water damage.
- Immediately notify management of the situation and call 9-1-1 if needed.
- Notify all personnel in the building of the situation and have them prepare to evacuate if needed.
- Personnel will evacuate if needed to a predetermined assembly area by department and will all be accounted for.

In the Event of an Earthquake

In the event of a major earthquake, follow the evacuation plan and look for shelter by followed supervisor instruction.

- See if the situation is okay, check yourself and the surrounding area for any injured persons or building damage.
- If life is at risk, or rescue is needed immediately called 9-1-1
- If there are any power lines exposed from damages incurred by the earthquake notify maintenance so the power can be turned off to help prevent any shock, or electrical fires from causing further damage.
- Immediately notify management of the situation and about any injuries or damages that were caused.
- Notify all personnel in the building of the situation and have them prepare to evacuate if needed.
- Personnel will evacuate if needed to a predetermined assembly area by department and will all be accounted for.

In the Event of a Fire-

If any type of fire event is happening, immediately follow the evacuation plan and leave the building by following supervisor instruction. Supervisor will be contacting for emergency help by using the emergency response contact list to stop the fire.

- See if the emergency can be contained by use of fire extinguisher first. If it is out of control find the nearest fire alarm and trigger the alarm and call 9-1-1.
- Immediately notify management of the situation, where the fire is at, and any team, or department that may be affected.
- Notify all personnel in the building of the situation and have them prepare to evacuate if needed.
- Personnel will evacuate if needed to a predetermined assembly area by department and will all be accounted for.

In the Event of Tornado

In the event of a Tornado within any of the three building facilities, the guidelines and procedures in this section are to be followed.

- As soon as a tornado is noticed or there is notification of a tornado prepare for the worst.
- Immediately notify management of the situation
- Prepare for shelter in place if necessary.
- Board up all the windows in the building and ensure that people stay away from any doors or windows.
- Ensure that emergency kits are distributed that include candles, a battery powered radio, blankets, water, and some food items that are nonperishable.
- Notify all personnel in the building of the situation and have them prepare to evacuate if able or needed.
- Personnel will evacuate to a predetermined assembly area by department and will all be accounted for if needed.

Write a nature-based test scenario (earthquake, mudslide, wildfire, several weather, tornado, flash flood, hurricane, volcano, etc.)

Earthquake Scenario:

Scenario: A powerful earthquake just hit Southern California lasting nearly one minute. In your area, you experienced significant shaking and unsecured objects have fallen onto desks, tables, and the floor. Power is out (except for areas on emergency generator power). Water is running, but pressure is noticeably low, and it appears cloudy. There are no apparent fires, hazardous materials spills, or other dangerous hazards in your area beyond fallen debris. Three staff members have sustained injuries from falling objects; however, all can continue to work. No other people have been injured. VOIP phones can dial internal extensions, but unable to dial external phone numbers. Several staff members have attempted to use their personal cell phones to make outside calls, but there is no signal. Computers plugged into red outlets, laptops and WOWs with battery power can access email and internet. Supply and equipment room floors are littered with items that have fallen from supply carts, including several pieces of equipment that have been damaged by falling to the floor. Some ceiling tiles have also broken loose and fallen to the floor.

Hurricane Scenario:

Monday, 8:00 a.m.: The National Hurricane Center reported that after a week in warm open waters, Hurricane Milo is approximately 200 miles off the coast of the Pacific. The local office of the National Hurricane Center issued a hurricane watch for large portions of the coast, including the Bay Area. Currently a Category 1 hurricane, Milo continues to gain strength and is projected to make landfall within 72 hours. Forecasters are already warning of the potential for this storm to become an extremely powerful Category 4 hurricane.

Wildfire Scenario:

Tuesday, 3:00 p.m.: The U.S. Forest Service spots a fire 40 miles outside of town. The fire is spreading rapidly, threatening numerous acres of forest, and moving in the direction of the Bay Area. Several buildings have already burned on properties outside of Bay Area; heavy smoke is reducing visibility and air quality, and a major electrical transformer is destroyed, causing widespread power outages. The local fire chief warns that at the fire's current rate of spread, it will reach residential and business areas within 24 hours if not contained. A mandatory evacuation is issued for the Bay Area, which includes Digi Knight workplace. Schools are closed and roads throughout the area are jammed with people trying to leave.

Flood Scenario:

The Event Early in the morning of March 15th, the National Weather Service Doppler radar indicates that thunderstorms producing heavy rainfall and damaging winds more than 60 mph are headed towards the Bay Area. By 9:00 a.m. that day, runoff from the heavy rain begins to flood low-lying areas in Freemont, CA, and the wind downs power lines, causing power outages throughout the city. By 5:00 p.m., the normally quiet creek has crested its bank, causing more flooding. The strong winds continue to knock down more power lines. There are reports that in some areas of Freemont (The Bay Area), people are trapped in their businesses and homes, many streets and roads are flooded, and there is concern for several homes that are located on a steep slope to the west of Freemont. Roads are closed, and the bridge that links the northern and southern parts of Freemont has been washed out. Power is out in many areas across the community.

Resources:

All departments have a Disaster & Emergency Response Manual (DERM), which is a thick red binder containing your department-specific disaster plan and other important resources. All staff should know where the binder is located, have access to it, and be familiar with its contents. Please take a moment to locate and review your DERM binder. All parties assigned to the roles will be available to participate in mock disaster. Also, conference rooms are available for table-top exercises.

Write a man-made-based test scenario (bomb threat, riot, power outage, chemical spill, evacuation, computer/data/network outage, biological threat, employee strike, etc.).

TO: Internal Test Team

FROM: Director of IT Operations

DATE: 7/15/2021

SUBJECT: Evaluation of Power Outage Response

I am writing to request an evaluation of our response to a major power outage. It is pertinent that we evaluate how our systems respond to a major long term power outage. This test must be run throughout the year to make sure our backup power systems are always operational.

To make sure our company is prepared for anything it is best to continuously test our systems to make sure they are operating at an efficient level to maintain our operation at any level. This would include the complete loss of power from the main power grid. If our backup power systems fail during a major power loss, we would face a potential loss of revenue in the millions depending on how long the power gird was out.

During this test, please make sure you test not only our backup generators, but also the intermediate backup batteries that would prevent a total outage before the generators kick on. We also need to test our fuel delivery system from the onsite fuel tanks that deliver fuel to the generators. Lastly, we need to train our employees on what is considered critical infrastructure at our company in the event we must stay on emergency power and drop non-critical systems to stay online.

Develop a plan to do a tabletop test of what would happen in the event of a mudslide.

Nature-Based Test Scenario:

In preparation for nature-based threats to DigiKnight corp. We will be conducting a mandatory test scenario to prepare for the event of an earthquake. Training for this event will include proper assessment techniques for determining damage after an earthquake which will including but not be limited to instruction on how to clear debris and remove equipment from any damage areas, how to stop all production equipment when and if necessary, and what steps to take to ensure safe practices while doing so. This training will also include instructions on how to contact and notify all high-level employees, maintenance teams, and other personnel in the event of an emergency. A drill will be conducted to assess the level of efficiency for the earthquake action plans reviewed in training sessions.

Thank you for your cooperation in this matter.

Man-Made-Based Test Scenario:

In preparation for man-made based threats to DigiKnight corp. We will be conducting amendatory test scenario to prepare for the event of a network outage. Training for this event will include procedures for notifying high level employees, IT teams, and other personnel, as well as how to determine the cause of an outage and the time frame for its recovery. This training will be broken down into several parts depending on the scale and time frame of each scenario outage. A drill will be conducted to assess the level of efficiency for network outage action plans that will be reviewed in these training sessions.

Emergency History-

In the space below, describe emergencies which have occurred. Include the date, the location within the building, the number of materials affected, recovery procedures, and the resources (time, money, personnel, etc.) needed for complete recovery from the emergency. Also note any vendors or suppliers used in recovery actions and evaluate their performance for future reference. This section should be updated after any emergency occurrence.

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

Damage Assessment Checklist-

How big is the damaged area?

What kinds of records have been damaged?

How long have items been wet?

Any signs of mold?

What team members/additional personnel are needed?

What supplies are needed?

Incident/disaster form

On-duty workers will make the initial inputs into this form after being notified of an emergency or catastrophe scenario. It will subsequently be sent to the ECC, where it will be updated on a regular basis.

This page will serve as a running journal until the incident/disaster has passed and "normal operations" have restored.

TIME AND DATE

____

TYPE OF EVENT

____

____

____

____

____

LOCATION

____

____
____

BUILDING ACCESS ISSUES

____
____

____
____
____

PROJECTED IMPACT TO OPERATIONS

____
____

____
____
____

Running Logs (ongoing events)

____
____

____
____
____

Create an assessment for determining inventory or list of critical resources at damaged site.

This assessment will have three different ratings for 3 different levels of situations to help accurately gauge the issue, and what needs to be done to resolve it. The first level, level 1, is the lowest damaging rating. When assessed a one, there are mainly minor with some medium difficulty fixes, and is light on the budget. A level 2 rating will be given in a situation in which the financial strain and problems are anywhere from low too high in cost and difficulty but can be averaged out to around medium. Finally, a level 3 rating will indicate that there is severe damage. The financial burden and difficulty for a level 3 assessment are remarkably high on the company and could lead to problems beyond the original such as downtime and finances. This assessment system provides a scale to help a business or company better prepare for a situation based of an initial canvassing.

Level One:

An example of a level one rating will be things such as power or network outages. These identify as a level one for several reasons. First, the economic responsibility is small, as the power or network outages are out of their control, the business just needs to focus on possible data corruption or data loss. Two, especially if a business is up to date on backups there would be little to no cost to them besides the downtime. There would be no cost for restoration for the company unless the issue was completely neglected. However, if the issue is neglected some costs, such as overheating/overcooling of equipment might come into play depending on location, since the room may no longer be a controlled environment.

Level 2:

An example of a level two rating would be anything that could cause an extended downtime and a medium high financial burden. Things that would be in this section could be flooding and tornadoes. These situations are likely to cause a lot of small damage, or one cluster of a lot of damage. The financial burden and downtime would correlate to how fast the situation is to get under control. Assuming something like a flood, the longer the components are under or near water the longer they must become damaged and unsalvageable. In this scenario, approximately half of the damaged resources may be able to have their data recovered, but most of the physical hardware would be destroyed.

Level 3:

A level three rating is the worst assessment and indicates major damage to the infrastructure and/or data loss. Examples of something that may cause this rating would be hurricanes and earthquakes, as they can be absolutely devastating. With a level 3 rating, the company will experience long amounts of downtime on that main site, almost forcing them to initiate a backup. Most of the equipment and data will be unrecoverable, and the financial loss would be devastating. A level three disaster could raze a company in one fell swoop if said company has not prepared for the disaster.

Media Communications-

Disaster Declaration Statement

System Failure at Digi Knight Technologies Inc

The following declaration statement was issued today by the Digi Knight Technologies Inc:

Located at 2725 E. Technology Ave, Freemont, CA 94536: At approximately 2pm there was what is currently being investigated as a catastrophic system
failure at Digi Knights Headquarters.

Whereas I, Carlton Smith, CEO & Founder of Digi Knight Technologies Inc am issuing a disaster declaration and am activating the Disaster Recovery Team. All disaster recovery team members must report immediately to their predetermined stations.

All employees will be contacted by their department heads via email and phone with further instructions.

All vendors, suppliers, contractors will be contacted by designated company liaisons.

All business partners will be contacted by their designated representative.

To all valued customers/stakeholders we will be fielding calls via a 1-800 number that is currently being setup. This number will be released within 6 hrs. via the local media.

The safety and well-being of our employees, contractors and neighbors is our priority. As more information is available, we will be providing updates through Digi Knight web site and regular media briefings.

Note for Media: Media briefings will be held at our alternate site at 1pm daily.

Sincerely yours,

Carlton Smith

Chief Executive Officer

<u>Resources-</u>

2019 Cyber Security Statistics Trends &amp; Data. PurpleSec. (2021, March 24). https://purplesec.us/resources/cyber-security-statistics/.

Comodo. (2021, June 1). What is Malicious Software?: Different Types of Malicious Software. Comodo News For Enterprise Security. https://enterprise.comodo.com/blog/ what-is-malicious-software/.

Data corruption and loss: causes and avoidance. (n.d.). http://www.thexlab.com/faqs/ datacorruption.html.

Kill, G. (2018, August 20). The 11 Leading Causes Of IT Downtime. Integracon. https://integracon.com/11-leading-causes-downtime/.

Mathews, R. (2021, March 25). Tips to prevent database corruption in web hosting server. Bobcares. https://bobcares.com/blog/database-corruption/.

Site Uptime Tips, T. (2019, December 20). 5 Common Server Problems and How they Affect Your Website. SiteUptime Blog. https://www.siteuptime.com/blog/2019/09/04/5- common-server-problems-and-how-they-affect-your-website/.

What is Malicious Software?: Different Types of Malicious Software. Comodo News For Enterprise Security. (2021, June 1). https://enterprise.comodo.com/blog/ what-is-malicious-software/.

Fremont, CA natural disasters and weather extremes. (n.d.). USA Location information - USA.com. https://www.usa.com/fremont-ca-natural-disasters-extremes.htm#:~:text=The%20chance%20of%20earthquake%20damage,lower%20than%20the%20national%20average

(EQ) Earthquake hazards of the Bay Area today. (n.d.). USGS Earthquake Hazards Program. https://earthquake.usgs.gov/earthquakes/events/1868calif/virtualtour/modern.php

(EQ) Housing Background Report- Earthquake Maps. (n.d.). City of Fremont, California. https://fremont.gov/DocumentCenter/View/2908/HS_web_pt2?bidId=

(FL) See your local sea level and coastal flood risk. (n.d.). Climate Central. https://riskfinder.climatecentral.org/place/fremont.ca.us?comparisonType=place&forecastType=NOAA2017_int_p50&level=3&unit=ft

(FL) Fremont, California. (n.d.). Flood Factor. https://floodfactor.com/city/fremont-california/626000_fsid#community_solutions

Map shows riskiest areas in California for damaging wildfires. (2021, June 3). ABC7 San Francisco. https://abc7news.com/fire-near-me-california-danger-map-wildfire/10733648/

A look at the Bay Area's history of tornadoes. (2015, May 15). Science. https://blog.sfgate.com/science/2015/05/16/a-look-at-the-bay-areas-history-of-tornadoes/

California has active and hazardous volcanoes. (n.d.). USGS.gov | Science for a changing world. https://www.usgs.gov/observatories/california-volcano-observatory/california-has-active-and-hazardous-volcanoes

Volcanoes. (2021, May 26). Plan Ahead for Disasters | Ready.gov. https://www.ready.gov/volcanoes

What is cold site? - Definition from Techopedia. (2011, July 31). Techopedia.com. https://www.techopedia.com/definition/998/cold-site

Crocetti, P. (2018, December 30). What is warm site? - Definition from WhatIs.com. SearchDisasterRecovery. https://searchdisasterrecovery.techtarget.com/definition/warm-site.

Reed, J. (2020, November 27). Comparison Of Disaster Recovery Sites: Which one to Choose? Official NAKIVO Blog. https://www.nakivo.com/blog/overview-disaster-recovery-sites/.

Spacey, J. (n.d.). *11 Elements of a Server Room*. Simplicable. https://simplicable.com/new/server-room.

https://www.seguetech.com/three-stages-disaster-recovery-sites/

https://www.omnisecu.com/ccna-security/types-of-backup-sites.php

Acronis. (n.d.). *3-2-1 rule of backup*. https://www.acronis.com/en-us/articles/backup-rule/

Aleks (NAKIVO). (2020, December 23). *A complete guide to backing up and restoring VMware ESXi host configuration*. Spiceworks Community - IT Best Practices, How-tos, Product Reviews, written by and for IT Pros. https://community.spiceworks.com/how_to/174408-a-complete-guide-to-backing-up-and-restoring-vmware-esxi-host-configuration

Tarsnap. (n.d.). Tarsnap - Online backups for the truly paranoid. https://www.tarsnap.com/

Veeam. (2017, August 9). *KB2328: How to backup vCenter server appliance*. Veeam Software. https://www.veeam.com/kb2328

Veeam. (n.d.). *VMware backup & replication software – Veeam backup & replication*. Veeam Software. https://www.veeam.com/vmware-esx-backup.html?ad=menu-products

Appendix A-

Communication Log

Date	**Time**	**Name of Contact/ Business**	**Communication Modality**	**Notes**

Appendix B-

BCDR Phase 7-9: Checklist – Disaster Recovery Specialist

Supplier Checklist-

1. **Who in the company is authorized to work with Suppliers?**

Admin Head - Mark Saunder – 415-555-8643

Research and Development Head - Carlton Bowden – 415-555-3223

Shipping Head - Kenneth Gilliam – 415-555-6431

Purchasing Head - Katherine Cavenaugh – 415-555-3298

1. **Who are the Key Suppliers for DigiKnights?**

DVD/CD/Cases Suppliers-

The Tech Geek – Primary Supplier.

Call – 1-800-456-0825

Address – 48965 Warm Springs Blvd, Fremont CA 94539

Disc Makers- Secondary Supplier.

Call – TOLL FREE – 800-468-9353

Call – Local – 856-663-9030

Address – 7905 N. Route 130, Pennsauken NJ 08110-1402

Dub-It Media Services- Secondary Supplier.

Call – 1-888-99DUB-IT

Call – Local – 323-993-9570

Address – 1110 North Tamarind Avenue, Hollywood CA 90038

ISSI Business Solutions- Secondary Supplier.

Call – TOLL FREE – 1-800-660-3586

Call – Local – 425-483-4801

Address – 22122 20th Ave SE #152, Bothell WA 98021

Box Suppliers-

Customized Packaging Solutions Inc – Primary Supplier.

Call – N/A

Address – 8333 24th Avenue, P.O. Box 278060, Sacramento, CA 95826

The Packaging House, Inc. – Secondary Supplier.

Call – 800-966-4594

Address – 6330 North Pulaski Road, Chicago, Illinois 60646-4594

Paper Supplier-

JC Paper – Primary Supplier

Call – 510-413-4700

Address – 47422 Kato Rd, Fremont, CA 94538

- **How to address Suppliers during a disaster?**

During an event, our suppliers will be one of the first groups to be notified of any disasters that could affect scheduled drop-offs off supplies and other situation where those suppliers would be involved. We do not want to send an influx of updates to these suppliers, and stress that we appreciate suppliers and driver's patience during the uncertain time. Suppliers, Clients, and other parties will be sent detailed business continuity plans for DigiKnights in a timely manner, as to let our supports know what is happening in the company, as well as who and want is affecting during an event.

- **How can the Suppliers contact the company during an event?**

We should direct Suppliers to contact our main phone line (415-555-2668) during a disaster. If an alternate number and address are created in the event of a new location for the company during said disaster, Suppliers will be notified as soon as those resources are set up. We want to assure Suppliers
that we appreciate their patience during this event and hope to continue their and the company's business connections.

Appendix C-

Scope

The Business Continuity Plan is limited in scope to recovery and business continuance from a serious disruption in activities due to non-availability of DigiKnight. The Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Strategy of this document. This plan is separate from Digiknight Disaster Recovery Plan, which focuses on the recovery of technology facilities and platforms, such as critical applications, databases, servers, or other required technology infrastructure. Unless otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations. The scope of this plan is focused on localized disasters such as fires, floods, and other localized natural or man-made disasters. This plan is not intended to cover major regional or national disasters such as regional earthquakes, war, or nuclear holocaust. However, it can provide some guidance in the event of such a large-scale disaster.

Purpose Since the company will be executing its work from two different locations, it is highly critical for Digiknight to come up with an updated and well tested Business continuity plan which can be implemented in any kind of calamity to perform the smooth running of business and customer satisfaction. If not, these calamities can cause a serious disruption in the running of business and a loss of revenue. The purpose of this plan will be:

· Have the hardware and networking in place for each system, to enable it to perform critical tasks independently in case second facility comes down.

· Understand and mitigate risks.

· Provide detailed plan of action in case of an incident.

· To have a data recovery system in place in case of system failures/crashes.

· Have cross training of resources in place to make it possible to find a proxy at other location in case of natural disaster at one.

Plan Overview the BCP can be achieved as follows:

· Each department will come up with its own risks and mitigation.

· IT Department will come up with Disaster recovery plan for hardware so that disruption can be minimized.

· Each team will have a critical resource appointed. (A person who is aware of all the workings of the team)

· A backup of data will be created, updated, and maintained regularly.

· Trial run of backup facility will be done for at least 1 weak to debug issues if any and ensure smooth running.

· Trainings will be performed for employees about what to expect and how to react in case of emergency.

· An alternate contact information will be given to customers in case primary contact is down.

Testing

Below are the types of testing necessary to make sure the quality of product (software) is maintained as well as other external factors are maintained. 1) Software testing -A rigorous test phase must be planned while creating the software where it is tested across a sample data set. Testing methodologies like black box testing, pre-prod system running etc. must be performed before making the software live. 2) Network and Server Testing- Networks should be tested for week points, sensors should be placed strategically in Demilitarized Zones, to alert system hack attempts, Intrusion Detection and Prevention Systems should be in place, there should be Risk Analysis done by checking resistance, recognition, and recovery capabilities of the system against hacking attempts. 3) Payment Gateway Security- Proper testing should be done to check if there is any week point in accessing payment gateway that can be manipulated by a hacker. Firewalls and Antiviruses should be tested by trying to hack the system. 4) Physical Building Security- Making sure security protocols are followed and access cards are working properly. It should be checked that no week points are left in the building security, CCTVs are working properly and strategically placed to avoid blind spots. 5) Backup Server and Network Testing- Making sure backup servers are as secured as primary servers and up to date. All the tests done for primary network and servers need to be carried out here as well. Also switching of load form primary to secondary servers should be tested for glitches and vulnerabilities.

6) Fire/Electric Hazard Testing- This cannot be tested but the quality of electric cables used should be of high quality as well as Fire extinguishers should be tested periodically and replaced if required.

Business Continuity Phases

1.Response Phase

· Perform an evaluation of degree of destruction caused to administration and business.

· Provide an update to management about the status and degree of destruction and losses.

2.Resumption Phase

· To provide necessary help and equipment to employees so that they can prepare themselves.

· Have focus groups to brainstorm on implementation of Recovery plans.

3.Recovery Phase

· To execute methodologies decided upon in the Business Recovery Plan.

· Co-ordinate with management to recognize duties for recovery teams.

· Co-ordinate with employees to guide them in their duties.

4.Restoration Phase

· Prepare the strategies to energize the development and movement of business operations after repairs and restorations.

· Manage the movement and relocation of resources.

Revisions-

Delivered on 7/18/2021.