**DigiKnight**

**Business Continuity Plan**

**Team CLP**

Version 1.0

8/8/2019

**Table of Contents**

[**DOCUMENT CHANGE CONTROL 6**](#_heading=h.30j0zll)

[**Section I: Introduction 7**](#_heading=h.1fob9te)

[**A.**](#_heading=h.3znysh7) **Introduction 7**

[**B.**](#_heading=h.2et92p0) **Objectives 7**

[**C.**](#_heading=h.tyjcwt) **Sections Summaries 8**

[**D.**](#_heading=h.3dy6vkm) **Assumptions 8**

[**E.**](#_heading=h.1t3h5sf) **Changes to the Plan/Maintenance Responsibilities 9**

[**F.**](#_heading=h.4d34og8) **Plan Testing Procedures and Responsibilities 10**

[**Section II: Threats 12**](#_heading=h.3rdcrjn)

[**A.**](#_heading=h.26in1rg) **Introduction 12**

[**B.**](#_heading=h.lnxbz9) **Natural Threats 12**

[**C.**](#_heading=h.35nkun2) **Man-made disasters 12**

[**D. IT and Technology-Based**](#_heading=h.1y810tw)

**E**[**.**](#_heading=h.2s8eyo1) **Environmental/Infrastructure Threats 14**

[**F.**](#_heading=h.e1q23le697eu) **Mission Critical 15**

[**G. Important**](#_heading=h.8tsitrfhic8h)

[**H. Minor**](#_heading=h.m38tr9ovuiyg)

[**I. Mission Critical Functions (Non-IT)**](#_heading=h.rkuiz0jvw0kv)

[**Section III:Backups 13**](#_heading=h.3whwml4)

[**A.**](#_heading=h.pkwifws41c51) **Backup and Restore Sections 23**

1. [**What data would be backed up**](#_heading=h.9unpu47yrmbo)
2. [**What data would be backed up to**](#_heading=h.t60qpm97rye)
3. [**Software used for the backup**](#_heading=h.czxc9oodc2nn)
4. [**Would the backup be incremental, full, or both**](#_heading=h.kp1z16krdvj8)
5. [**How long would the backup take based on the method of replication**](#_heading=h.i14cba4uudf0)
6. [**What is a good method of backing up the vCSA appliances**](#_heading=h.mqq5ol8569bh)
7. [**Cost of Cloud vs On-Premise**](#_heading=h.kspnbjamhj0p)

[**Section IV: Insurance 23**](#_heading=h.4f1mdlm)

[**A.**](#_heading=h.19c6y18) **Insurance Information 23**

[**B.**](#_heading=h.9s892r5wr49l) **FEMA Continuity Guidelines** [**23**](#_heading=h.19c6y18)

[**Section V: Backup Sites 38**](#_heading=h.1mrcu09)

[**A. Activate Alternate Work Sites 23**](#_heading=h.setazc31ecg6)

[**B.**](#_heading=h.nk9llnny8bng) **Alternate Work Site Plan 23**

[**C.**](#_heading=h.t37rn86e2mnf) **Cold Site Plan 23**

[**D.**](#_heading=h.4zhf8t7puao) **Warm Site Plan 23**

[**E.**](#_heading=h.1h787qk88gab) **Hot Site Plan 23**

[**F.**](#_heading=h.clf4mrbkwzd7) **Mobile Site Plan 23**

[**G.**](#_heading=h.3yy1k6bz7c12) **Mirrored Site Plan 23**

[**H.**](#_heading=h.4n8zdggbh0sp) **Active Disaster Procedures 23**

[**Section VI: Emergency Contacts & Event Templates**](#_heading=h.u2w2fj1ravqr)

[**A.**](#_heading=h.26gdwsju7y6v) **Emergency Contact Information & Procedure** **38**

[**B. Event Templates**](#_heading=h.bboho2nfshrx) **38**

[**Section VII: Testing Procedures 38**](#_heading=h.uw6q5h62zl6j)

[**A.**](#_heading=h.8wji7muzrax4) **Alarms** **38**

[**B.**](#_heading=h.3je6acfmez7c) **First Aid Supplies & CPR 39**

[**C.**](#_heading=h.lsz2x6ivzv78) **Fire Suppression Equipment** **38**

[**Section VIII: Evacuation Procedure 38**](#_heading=h.73d57kzeqali)

[**A.**](#_heading=h.pkoaabe51k7i) **Evacuation and Safe Space Plan** **38**

# DOCUMENT CHANGE CONTROL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Requester** | **Tech. Writer** | **Change/Review** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Modified by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_/\_\_\_\_/\_\_\_\_\_

Reviewed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_/\_\_\_\_/\_\_\_\_\_

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_/\_\_\_\_/\_\_\_\_\_

# Section I: Introduction & Section Summaries

## Introduction

In the event of a disaster which interferes with DigiKnight’s ability to conduct business from one of its offices, this plan is to be used by the responsible individuals to coordinate the business recovery of their respective areas and/or departments. The plan is designed to contain, or provide reference to, all of the information that might be needed at the time of a business recovery.

## Objectives

The objective of the Business Continuity Plan is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a facilities (office building) disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

**A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization’s ability to deliver essential business services.**

**The priorities in a disaster situation are to:**

1. Ensure the safety of employees and visitors in the office buildings.
2. Mitigate threats or limit the damage that threats can cause.
3. Have advanced preparations to ensure that critical business functions can continue.
4. Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.

The BCDR Business Continuity Plan includes procedures for all phases of recovery.

## Section Summaries

**Section I, Introduction & Section Summaries**, contains a brief introduction of the document and its purpose. This section also contains brief summaries of each section.

**Section II, Threats,** describes the threats that may affect DigiKnight. These threats include natural disasters and man-made disasters. The section also defines some scenarios and their likelihood. The section rates some risks and defines DigiKnight’s mission critical departments.

**Section III, Backups,** describes DigiKnight’s backup options and defines the company’s backup procedure. This section compares the prices of having an on-premise backup system vs. paying for an AWS instance that can handle our backups.

**Section IV, Insurance,** talks about the different types of insurance DigiKnight needs and how much it would cost the company.

**Section V, Backup Sites,** describes the different types of backup sites that DigiKnight can use. This section also talks about active disaster procedures, this includes what documents need to be saved and what management and the BCDR team need to do.

**Section VI, Emergency Contacts & Event Templates,** contains emergency contact numbers and the procedure used to contact them if needed. The second part of this section contains templates that can be used for recording information and used to record proper procedure use.

**Section VII, Testing Procedure,** describes DigiKnight’s emergency assets and the proper way to test them. The section explains the procedure and the time frame that should be used for each test.

**Section VIII, Evacuation Procedure,** contains the proper evacuation procedure that should be taken during an emergency. This section includes an evacuation plan, the building’s utility plan, and a floor plan that shows inside assembly areas alongside emergency supplies.

## Assumptions

The viability of this Business Continuity Plan is based on the following assumptions:

1. That a viable and tested IT Disaster Recovery Plan exists and will be put into operation to restore data center service at a backup site within five to seven days.
2. That the Organization’s facilities management department has identified available space for relocation of departments which can be occupied and used normally within two to five days of a facilities emergency.
3. That this plan has been properly maintained and updated as required.
4. The functions and roles referenced in this plan do not have to previously exist within an organization; they can be assigned to one or more individuals as new responsibilities, or delegated to an external third party if funding for such services can be arranged and allocated.

## Changes to the Plan/Maintenance Responsibilities

The BC\DR plan should be altered as needed but should be completely updated on a 6-month basis. Some items on the plan can be left the same if no improvements are available. Meetings set-up every 6 months to review the plan and discuss changes will be arranged. These meetings will be comprised of managers, administrators, and BC\DR team members. . . An email used for recommendations will be set-up for staff to use. These recommendations will be reviewed during meetings. The following process are examples that can be used:

**Example #1:**

1. Everyone in the meeting is given a copy of the current plan.
2. The members will go over each section in order and will discuss whether changes are needed or left alone.
   1. Each member will vote on changes and will be given a chance to speak if needed.
3. Email recommendations will be voted on and implemented if approved.
4. A final review of the plan will be done with a final approval to all changes made.

**Example #2:**

1. The BC/DR team is tasked with creating a checklist of changes that should be made to the plan alongside new items that should be added. This should be completed before the meeting
2. Everyone in the meeting is given a copy of the current plan and a copy of the checklist.
3. BC/DR team goes over the checklist and talks about why these changes need to be made.
4. Email recommendations are voted on and each member has a chance to discuss anything they think should be changed or added.
5. All ideas from step 4 are voted on and reviewed before final implementation.

## Plan Testing Procedures and Responsibilities

BCDR management is responsible for ensuring the workability of their Business Continuity Plan. This should be periodically verified by active or passive testing.

# Section II: Threats

## Introduction

With multiple threats affecting a company it is essential that they are divided into their respectable categories: **Natural threats, man-made threats, and IT threats.** By dividing these threats we can then identify what impact they can have on your company. We will first identify these threats and identify the impact it will have on your organization. We can then proceed to mitigate and prevent these threats.

## Natural Threats

**Water Damage**

**Threat Sources:** Water damage can be caused as a result of many things. Could relate from a bad rain storm or could be caused by something man made, such as a broken water pipe or water that someone never cleaned up.

**Threat Level:** Water damage can cause a lot of costly repairs and maintenance to be made. Water damage can be prevented by keeping the building and surrounding areas up to date with the legal code and having mandatory meetings.

**Impact:** The impact to his organization for water damage can be very dangerous. Water can cause manufacturing lines to go down or even our server rooms. Water damage may also cause health problems with our employees so we need to be able to take precautions to prevent water damage in the future as it is vital for this company.

**Earthquakes and Landslides**

**Threat Sources:** Due to earthquakes having a wide range of strength of the tremors, it is difficult to gauge how much damage will occur in the future. They can range from minor shakes that might knock over light items on desks to resulting in buildings collapsing. Some of the more serious sources of damage can occur from structural damage, windows breaking over employees, machinery falling over, ceiling tiles falling, landslides, and building collapse. On the lower end, the most damage caused would be items falling off walls and desks. Another potential damage earthquakes can cause would be landslides. Landslides could affect the distribution of our products as well as affect our manufacturing process by affecting our suppliers.

**Upstream loss:** Losses can occur from companies we depend on to release our product. If the game developers experience a higher strength earthquake, the games they are releasing could be postponed or even completely lost in the destruction of their buildings. In the case of our other suppliers, our manufacturing resources could be affected in turn, taking a hit to the company revenue. If one or all of our case suppliers, DVD providers, box suppliers, or paper suppliers gets affected by an earthquake or the route that it takes for their products to reach our manufacturing building, our revenue will take a hit. Landslides could also affect our suppliers rate of providing materials required for production and the rate of distribution due to cutoffs of key highways and roads for distribution routes.

**Downstream loss:** Since the company has to distribute the product across the country, any earthquakes affecting shipping routes and locations where our products are being shipped to would affect revenue. Shipping could be stopped completely across some areas while in other cases only being delayed a few hours to a few days potentially. Landslides could also affect the company’s distribution across the country. If major highways and routes get blocked off by landslides, distribution could be slowed to the point where sales take a hit. Our key suppliers could also be affected, affecting our production rate, in turn affecting our distribution rate.

**Likelihood of occurrence:** Overall there is over a 99% chance that California will have an earthquake on a greater scale than a 6.7 in the next 30 years. However, our headquarters located in Fremont, California is 76% likely to experience an earthquake on a magnitude of 7.0 in the next 30 years. Landslides while being caused by earthquakes also have other precursors that could lead to the natural disaster such as flooding, heavy rain, and steep slopes. The areas most likely to have landslides would be areas near the Rocky Mountains, the Appalachian Mountains, and areas subject to intense rains and hurricanes along the east coast.

**Likelihood and vulnerability:** Our CD case and DVD case suppliers in California are also likely to be on the receiving end of a higher magnitude earthquake as well. Our suppliers in Hollywood are at a 75% chance of experiencing a 7.0 magnitude earthquake or higher within the next 30 years. Our other supplier in Fremont is at the same risk as us at a 76% chance to be affected by an earthquake greater than a 7.0 magnitude in the next 30 years.

Our box suppliers located in Sacramento are likely to be affected by an earthquake with a 76% possibility of a 7.0 magnitude or greater within the next 30 years.

Our paper suppliers are also likely to be hit by an earthquake with a 76% chance of having a 7.0 or greater earthquake within the next 30 years.

With several vital clients being scattered throughout California, we have to expect potential loss as well. One of our clients in Redwood City, two clients in San Francisco, and another client in Sunnyvale are all at a 76% chance of experiencing an earthquake over a magnitude of 7.0 within the next 30 years. Our other two critical clients located in Santa Monica and Calabasas Hills are at a 75% chance of having a 7.0 or greater earthquake in the span of 30 years.

Landslides caused by earthquakes and water are not likely to directly impact a shipment by damaging the distribution vehicle. However, landslides could affect routes that are taken by distributors, affecting shipment time by a few hours to potentially even a day or more. In the case of our suppliers shipments of products required for manufacturing the final product, it could affect our production rate by multiple days due to the delay to ship out a complete product shipment.

**Impact of threats:** Impacts can range from nothing to complete disruption of business. Suppliers production being interrupted could affect our production rates and our distributors being slowed or stopped could affect revenue. Also any critical clients being affected by higher scale earthquakes can stop sales completely as areas try to recover from damage. Landslides would most likely affect the distribution of our products as well as the time we receive supplies necessary for production. Impacts could range from hours to days resulting in lost revenue by late shipments of completed products or slowing our manufacturing process.

**Flooding:**

**Sources:** Flooding is a common occurrence in California and can cause catastrophic damage to buildings and it’s interior. Of course this poses a huge risk for electronic and power equipment, the loss of life, and structural damage. These raging waters can literally drag a building off of it’s foundation

**Threat level:** California is highly prone to floods, in fact every county in California has been declared a flood disaster area. It is estimated that upwards of 580 billion dollars worth of structures and their contents are vulnerable.

**Company Impact:** The damages that floods may bring can be irreversible, potentially threatening to completely wipe out all operations in the event of a flood that is capable of washing away our building. This of course also poses a risk to the very lives of employees as well. In the best case scenario we can expect minor structural damages, and major structural damages to electronics, paper records, power sources, this may put our home office out of commission for several months, incurring further costs to relocate and attempt to continue operations.

**Wind Damage:**

**Sources:** Wind damage would damage caused as a result of high winds. This can just be winds affecting the building, winds blowing a tree down and into the building, or objects flying into/onto the building

**Threat Level:**

* High speed winds tend to occur around Southern California, more, thus it is not as much a worry as other disasters might be.
* The threat increases if there are tall trees around the building.
* The threat increases dependent on how near a rocky shore the building is.

**Company Impact:** The costs incurred by wind damage can range from minor property damage to building repairs. Server rooms are expected to not be near the perimeter, thus it will not take down servers. It could, however, impact the air conditioning of the server room, which would slow the speeds of company processes. This means that we will need a backup AC unit or for it to be protected by other means. Otherwise, costs will only be in building repairs, and a drop in company physical security during the times of repair.

**Fire:**

**Source:** The source of fire would be dry plant matter. Area that have droughts and low rain would have dense about of dry plant matter. It can also be caused by volcanoes and lightning strikes nearby.

**Threat Level:**

* Damaging the building and area.
* Damage increases if dry plants are nearby.

**Company impact:** Can stop and destroy the company building. It could destroy all servers and progress of the company if the data is not stored elsewhere.

**EMPs:**

**Sources:** Solar flares are caused by the sun. A relatively well known example is the [Carrington Solar Flare of 1859](https://owlcation.com/stem/massive-solar-flare-1859). These cause power grid disruptions, this may cause power issues and could result in an EMP on the building. Some scientists predict that these kinds of flares occur [once every 350 years](https://www.dailymail.co.uk/sciencetech/article-3198285/Is-Earth-hit-SUPERFLARE-Scientists-calculate-massive-solar-outburst-due.html). Alternative sources could be from terror attacks, acts of war, and anything else appears to be unlikely enough to not worry about.

**Threat Level:**

* Low, possibly the lowest, threat dependent on company location
* The company is very vulnerable to this kind of disaster, however, the most likely, natural cause is a solar flare; these don’t occur often.
* Dependent on the building’s structure, company practices for when devices are not in use, and time of occurence; the effect of an EMP could be range from just taking down servers to taking down all of the company’s electrical devices.
* No cold storage nor powered-down device loss.

**Company Impact:** Considerations may be made for encasing servers into a Faraday cage, or EMP resistant technology might be used by accident. Anything moe is unlikely to actually be enacted in response to natural EMPs. If a solar storm the size of the 1859’s is predicted to occur, this may change.

**Power outage:**

**Threat sources:** The source of the power outage would be multiple things from a powerline down that connected the company to the power, to the electric company generator losing power and shutting down causing a power outage for the company. A down power line is not very probable cause as most powerline are now underground hidden from view and from harm, unless an animal or natural causes from a natural disaster would happen.

**Upstream loss:** a power outage would stop all work on electronic devices. Stopping all progress on all works, also any unsaved work will be lost too causing progress on all work to be set back by an hour or a day if there is no ups or back up generator for the company.

**Likelihood:** 5% chance of happening

**Likelihood and Vulnerability:** This will be an unlikely thing to happen to the company but can be prepared for by having UPS backup on the servers and computers vital to the company.

**Threat Impact:** This will cause all progress to be lost for the timeframe the power is out and all unsaved work will be lost for the company. If any online services are available they will be down for the company. If a ups is available it will be hooked up to vital parts of the company or items that have not saved yet to minimize loss. A notice will be on the online services that it will be down for a bit until further notice.

## Man-made disasters

**Stolen/Lost/Damaged Company Property:**

**Source:** The internal threat that may come from our own employees is not one that should be ignored under any circumstances. We must of course be prepared for the dangers of company property being lost, stolen or damaged.

**Threat level:** The chances of company property being stolen by an employee should be considered mild, while workplace crimes cost upwards of 50 billion a year across the US, being in such a small organization this is not the biggest concern just must not be cast aside. There will always be the issue of people losing something, flash drives, papers, phones ect. Human error will always be in the mix and should be considered a high threat. Finally damaged property, this particular one is the least likely of the three since everyone here are responsible adults, but should be considered nonetheless. Employees may drop a company computer/laptop or burn out a computer part, or even spill liquid on expensive machines.

**Company impact:**

* Stolen Property, while it is unlikely that materials will be stolen from this small organization, considering that it is much easier to track for us, this is an issue that may arise at any time. Corporate credit cards could be stolen, cash drawer money could be stolen, hardware could be stolen ect. It is estimated that embezzlement costs companies across the US over 50 billion dollars a year. This can even cost extensive legal issues as well.
* Lost Property, in the even of property being lost the best case scenario will be that we lose a few hundred dollars laptop, or phone. This damage could be far greater however if these devices are containing sensitive information, damage to our reputation can not be tolerated. Extensive IT policies are to be put into place to minimize losses if an electronic device is lost.
* Damaged Property, this will mostly incur costs of repairs, of course it should be noted that only the most necessary of repairs should be approved. Damages can be a result of employees or nature. In the case of out employees, it is expected that all employees will take care of their materials, although they shall not be expected to repay repair costs, except for the most extreme of damages. In the case of nature, these damages are expected to be more pressing and can quickly incur heavy costs if precautions are not taken.

**Active Shooters:**

**Source:** The source/cause of an active shooter can vary greatly depending on your political stance on this controversial issue. Some think the gun is at fault and some think the human is at fault. One thing can be said for sure, active shooters are a result of anger and/or mental illness in an individual, combined with access to arsenal.

**Threat level:**

* Very low threat.
* DigiKnight has armed guards attending each of its buildings, greatly mitigating this risk.
* Also helpful that DigiKnight has few on-site employees, with plenty of places to hide between the three buildings.

**Company impact:**

* In the event of an active shooter successfully getting past the guard at any company building, company losses could be detrimental.
* Employee life could be lost, losing valuable resources for DigiKnight, along with reparation costs for affected families.
* Possible damaged equipment from missed bullets, or even worse sabotage if that is the shooter’s intentions.
* This is still unlikely to cause as much damage mentioned, as DigiKnight employs professional armed guards at each building to protect from instances such as these.

**Social Engineering Attack:**

**Threat Source:** Social engineering notably had become a very common attack against enterprises and small businesses and perhaps growing more in its sophistication with how it operates. Hackers had learned to be dynamic with many genius ways that are being used to fool employees and other individuals from businesses to hand over confidential data and sensitive information.The most common of social engineering attacks involve the use of emails and other communication mediums to cause a sense of urgency, fear and or other similar emotions to victims. This is also known as Phishing and according to the online article, 90% of data breaches come from phishing, ("Social Engineering Attacks: Common Techniques & How to Prevent an Attack," 2019). Phishing in the category of social engineering scams comes in many forms including Banking Link Scam, Fax Notice Scam, Dropbox Link Scam, Court Secretary Complaint Link Scam and Facebook Message Link Scam. The use of social engineering mostly involves humans as the element hence fighting against this can be very dicey.

**Upstream Loss:** The upstream occurrence of Social engineering attacks against key supplier of a company like DigiKnight would very much affect the quality of the service to their customers.

**Downstream Loss:** The downstream effect of such occurrence on the other hand would be the hardships and disappointments for customers of google who are to deal with losses because of their inability to provide quality services. DigiKnight like any other company can be susceptible to this type of threat.

**Likelihood of Occurrence:** The likelihood of occurrences for employees of an organization or a business like DigiKnight as potential victims of social engineering attack should never be taken lightly. According to the online article, 97 percent of social engineering attacks leads to malware that is capable of fooling users for their information ("Social Engineering Attacks: Common Techniques & How to Prevent an Attack," 2019).

**Impact of Threats:** This would affect the business operations of Digiknight due to mass compromisation of credentials and other sensitive data information. Compromised identity of Digiknight users would also affect productivity and growth.

**Mishandled drinks:**

**Source:** Mishandled drinks near expensive server or data equipment can be dangerous. The cause of this is lax policies or enforcement of said policies within a company, and the clumsiness and ineptitude of involved employees.

**Threat level:**

* Low risk
* Common knowledge, and company policies, should keep every employee informed that carrying drinks around expensive computer equipment is dangerous and prohibited.
* With the small amount of employees, this has less chances to happen.
* In the event that this does happen, it is likely that only one CPU would be damaged.

**Company impact:**

* Generally, low company impact, unless this is a common occurrence, and if it is common, then disciplinary actions must be carried out.
* The largest possible company impact would be if a drink was spilled on the main server shelf, or tossed into a production machine, but this is still unlikely.
* Company impact may be kept little-to-none by enforcing strict drink and food policies for all employees.

**Employee Error:**

**Threat Source:** Your employees are a liability, you may have guidelines and regulations in place, but employee mistakes are ranked as a top threat to sensitive data (Ncipher, 2019). Falling victim to social engineering, phishing, bribery, and other threats that could lead to data loss or hardware failure. Human error is inevitable, we are not perfect, so knowing how to train your employees to prevent further or future troubles is important.

**Upstream Loss:** DigiKnight communicates with video game companies to distribute their games. Misunderstandings and incorrect information can lead to productivity and trust loss. Incorrect data input and record keeping mistakes could also lead to trust issues with video game companies.

**Downstream Loss:** Our CD making process is regulated and maintained by employees. Problems caused by employees can lead to hardware malfunction or failure, causing the company money, trust, and productivity loss. Improper data input can also cause problems if not corrected in time. Employees must understand that the product is not for sale yet and disclosure of the product can lead to a breach in NDA’s. Any other hardware problems caused by employee can be considered loss if applicable.

**Likelihood of Occurrence:** As stated before the number one risk in a company is employee mistakes (Ncipher, 2019). 90% of data breaches involve human error (Kelly, 2017). This statistic does not even take into account voluntary attacks, because we are talking about mistakes/errors.

**Likelihood and Vulnerability:**

* 90% of data breaches involve human error (Kelly, 2017)
* The number one risk to a company is the employees (Ncipher, 2019)
* Humans make mistakes that is an inevitable problem.

**Threat Impact:** Employee mistakes can cause the company hundreds to thousands of dollars, depending on the offence. Data breaches can be caused by employee mistakes, social engineering targets these vulnerabilities. Hardware failure can be caused by human mistake, causing a loss in money due to replacement/fix costs. It can even cause data loss which could hurt the trust and reliability our clients have with us.

## IT and Technology-Based

**DDoS Attack**

**Threat Source:** DDoS attacks usually come from a person controlling a botnet designed to overload a server with requests for service. In doing so, the server will be overloaded with requests that it will usually crash. A DDoS attack could cause a lot of financial damage to the DigiKnight servers.

**Upstream Loss:** If DigiKnight is affected by a DDoS attack, they cannot access their servers to do their work.

**Downstream Loss:** DigiKnight’s customers servers could be affected by DDoS attacks which would stop them from doing any work or sell games so DigiKnight will end up losing money.

**Likelihood of Occurrence:** DDoS attacks are not uncommon nowadays, they are also not very hard to do. A recent study by Kaspersky Lab showed that DDoS attacks can cost companies over $1.6 million dollars in revenue.

**Likelihood and Vulnerability:** DDoS attacks should be a high priority for companies to protect against because they can happen so easily.

**Impact of Threats:** DigiKnight and their suppliers could be affected by DDoS attacks which could cost both parties a lot of money.

**Malware**

**Threat Source:** Malware can come in many different forms, if it can get onto a system or a network it can cause a lot of damage. It can delete important files on a system that can significantly slow production of a company.

**Upstream Loss:** If DigiKnight’s network or systems were affected by malware, it can halt their production and cost the company a lot of money. It could slow down the production of their plans to make more CD/DVD disks for their suppliers.

**Downstream Loss:** Malware could cost DigiKnight a lot of money if the malware is allowed to spread across multiple systems. The average cost of malware that a company is affected by is $2.4 million dollars.

**Likelihood of Occurrence:** Malware is a common threat in the cyber security world. The average time it takes to get malware of a network is around 50 days. That is a long time that a company can be affected by malware.

**Likelihood and Vulnerability:** No network is completely safe from being attacked, and companies often think they are immune to having malware get onto their systems.

**Impact of Threats:** DigiKnight could have their systems be down for more than a month if they do not use best practices for protecting their network against malware attacks.

**Malicious Links**

**Threat Sources:** With Javascript being one of the most popular languages used in web development.”JavaScript is currently being used by more than 94 percent of all the websites. (Toledo, 2018)” Malicious actors can hide malicious links on the web page that is served to the client or they can even disguise trojans as innocent links to bait a user to click on them. The client then proceeds to click on the link and has now given the actor access to their system or access to personal information.

**Upstream loss:** With the high dependability on their network infrastructure a malicious lnk could potentially compromise the network thus causing multiple interruptions throughout. WIthout networking there is no access to external data: game data, order data, customer information,shipping information, A Malicious link could lead to affecting multiple departments including but not limited to: finance dept, shipping sept, manufacturing dept, data storage dept.This could cause a potential problem when you have offices located in other areas.

**Downstream loss:** If systems within the network infrastructure becomes unavailable it could potentially lead to interruptions within the company. Internal networks will not be able to communicate meaning the servers will not be able to communicate with the workstations or network printers. With disc writing and printing being the company's focus losing internal communications can cause the company panic.

**Likelihood of occurrence:** Malicious actors are always looking for vulnerabilities and creating some as well. Userscan fall victim to some of these malicious links and at times the web server provider can fail to install patches leaving their system vulnerable to the latest zero day. A new threat by the name “form jacking” can steal information from a customer and the customer will not be able to tell the form they filled out was legit.

**Likelihood and vulnerability:** The malicious actor must first conduct research by stealing cookies from a user to send them a link that the user will be baited to click on. Social engineering can result in users clicking on these links. According to Verizon.com they claim that 92 percent of malware is delivered by email. With open source tools like Cuteit anyone with basic knowledge can create a malicious link.

**Impact of threats:** Usually a malicious actor attacks for monetary reasons and if a system is compromised due to a malicious link the attacker will more than likely ask for money in return. Rendering their network due to a malicious will cause the company to lose millions.

**Ransomware**

**Threat Sources:** In the most recent attack Baltimore has been infected by ransomware. The ransomware dubbed ‘Robbinhood’ has caused the city a reportedly $18.2 million (Duncan, 2019) .

**Upstream loss:** Ransomware utilizes encryption and locks out the user from the system or from accessing important files. This can affect communication with outside sources and with fear of the ransomware spreading the machines must be disconnected from the external servers to mitigate damages.

**Downstream loss:** When the internal network gets encrypted a timer is usually set by the attacker. If the victim fails to pay they will delete the files in question. This will result in huge losses for the company hours of work lost.

**Likelihood of occurrence:** There have been multiple ransomware attacks and there is an increasing amount of these attacks. Multiple cities and companies have felt the damage ransomware can cause.

* A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021. (Source: Cyber Security Ventures)
* 1.5 million new phishing sites are created every month. (Source: webroot.com)

**Likelihood and vulnerability:**

* Ransomware attacks have increased over 97 percent in the past two years. (Source: Phishme)
* A total of 850.97 million ransomware infections were detected by the institute in 2018.
* 34% of businesses hit with malware took a week or more to regain access to their data. (Source: Kaspersky)
* In 2019 ransomware from phishing emails increased 109 percent over 2017. (Source: PhishMe)

**Impact of threats:** Ransomware demands payment and at the same time encrypts the company's files and important resources. At times if the company fails to pay then the data can be lost and important information can be stolen. Falling victim to Ransomware can cause a company millions

* “The Erie County Medical Center (ECMC) in Buffalo, NY, last July estimated it spent $10 million responding to an attack involving a $30,000 ransom demand”(Vijayan, 2018)
* Cybersecurity Ventures, which pegged ransomware costs at $325 million in 2015, last year estimated damages at $5 billion in 2017 and predicted it would exceed $11.5 billion in 2019.

**Zero day Attack**

**Threat sources:** The threat source would be from the company developing the software and a user finding it, and could have it could affect the use of the software . The best way to stop a zero day attack would be to patch it or finish the software before releasing the software. If a zero day exploit is found by a person willing to tell about it, it can be fixed before anything bad can happen with it minimizing public reputation with the zero day. If a zero day attack is found and made public it should be patched and fixed immediately

**Upstream loss:** This can range from attacks on the company or on users. This would be bad for the company as publicity as the software is not safe to use, making the software sales go down.

**Downstream loss:** If a zero day exploit is used to attack users it could lower sales of the software. Until patched the known glitches should be inspected by known reputable tester for glitches and exploits.

**Likelihood:** There will always be a zero day exploit in a software. Preventing one from being used to harm others or exploit the system should be high up on the list of things to do. The best way to prevent one is to have the software updated to prevent known ones from reoccurring

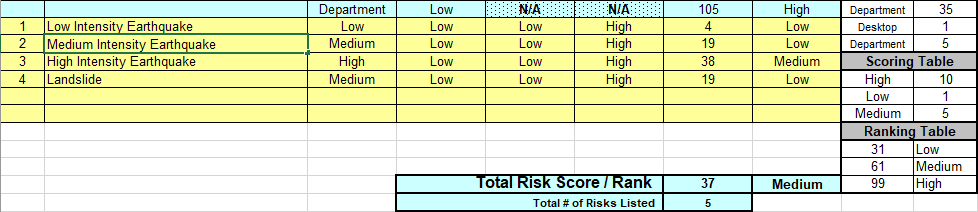
**Likelihood and Vulnerability:** There will always be zero day attacks even when the software has been out for a long time and most known zero day attacks are found. This can affect the system in unexpected ways and be used to harm users of the system. They can be prevented by knowing about the zero day but knowing about the zero day attack will be hard.

**Threat Impact:** The threat impact of a zero day attack could be that the public knows about the safety of the product. This will hurt the software sales, and the trust of the users and stockholders.

## Environmental/infrastructure Threats:

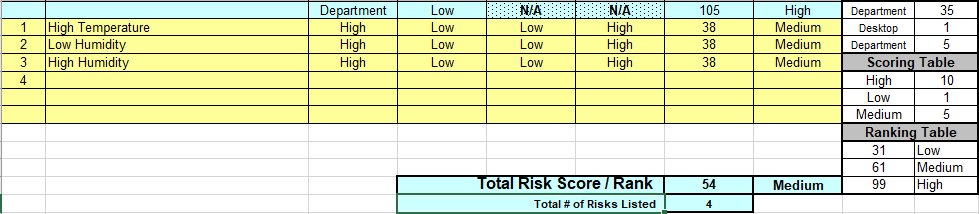
**Building Structure:**

WIth our company located in California, there is a threat of an earthquake potentially damaging the building structure. It’s expected that in Fremont, there is a 76% chance of an earthquake around a 7.0 on the magnitude scale within the next 30 years. Generally, earthquakes within the 5.0 and 6.0 scale have light damage to buildings, while anything above a 6.1 are more likely to inflict damage, and anything above a 7 having guaranteed damages. In the face of a high scale earthquake machinery falling or being damaged would be the greatest impact. Another potential threat caused by earthquakes would be nearby hills experiencing rock slides or landslides due to the earthquake. With enough impact from either source, machinery and buildings could be damaged or completely blocked off. Significant structural damage would result in upstream loss in the form of lost productivity in our research and development team, our marketing department, our sales department, and our shipping department. Our Shipping department would also be a downstream loss, as well as our manufacturing department.



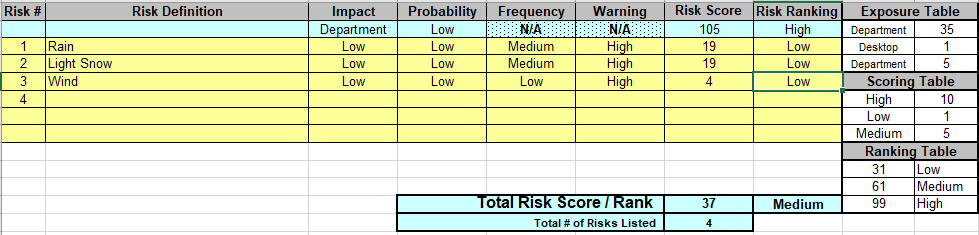
**Environmental Damage to Machinery:**

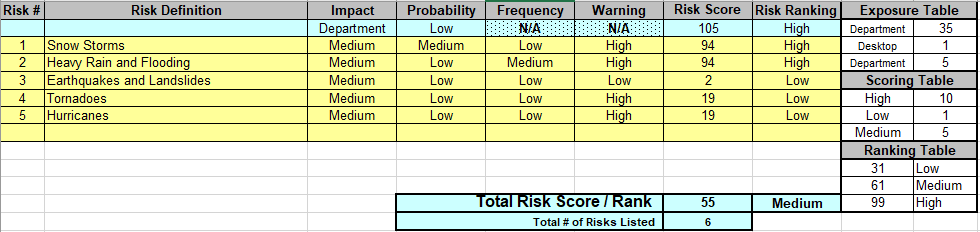
The environment within the server room and the production facility are a potential risk for production and continuity of the different departments. The ideal temperature range for computer equipment is within 68 and 75 degrees fahrenheit. Server rooms and production rooms should avoid having any temperatures exceeding 85 degrees fahrenheit. Humidity should also be considered for the ambience of the server rooms. Ideally, humidity levels should be within 45% and 55% in order to have reliable continuity. Lower levels of humidity leave equipment at risk of electrostatic damage while having too high of humidity can cause water condensation resulting in corrosion, earlier component failure, and earlier system failure. Dependant on which systems fail, there are potential losses for both upstream and downstream. Machinery for production being damaged or stopped by environmental damage could result in downstream loss. Different servers and networking equipment being damaged or stopped could result in upstream losses by different departments involved in coordinating with clients and suppliers being slowed or stopped.



**Natural Disasters Affecting Production & Distribution:**

Weather is another consideration for environmental threats. Extreme weather could completely halt product distribution as well as delaying the arrival of products required for manufacturing. This delay on production could also lead to a delay of our distribution rate. Overall crucial highways being blocked off. Slower distribution time due to driving at a slower velocity. Some extreme weather that could affect the distribution of our suppliers and ourselves would include snowstorms, floods, earthquakes, and on the less frequent side tornadoes, hurricanes, and landslides. Calmer weather that would affect distribution rates would be rain, light snow, and winds.



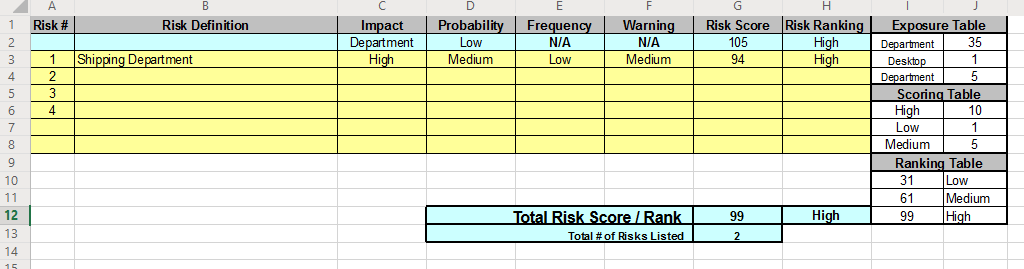


## Mission Critical:

**Shipping department (getting products ready for shipping and sent out; receiving**

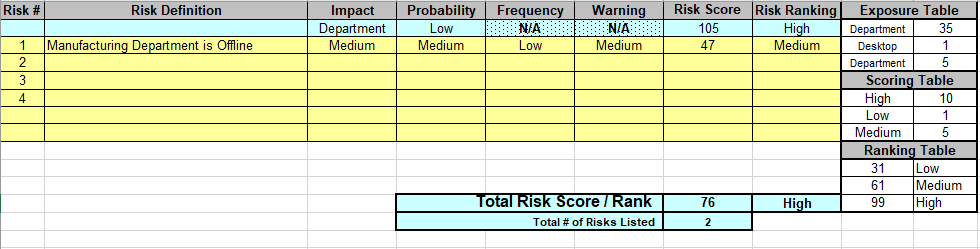
**shipments of supplies for production):**

The shipping department is a mission critical resource as Digiknight depends on shipping and receiving in order to make a profit. If the shipping department was to fail, then the company would take a huge loss. DIgi knights needs to be able to ship out orders to their customers and receive materials such as (blank discs if outsourced, products needed to make the discs, and other materials). The company cannot afford to lose shipping because losing shipping means losing customers and we are not in the business of losing money. If shipping is affected due to the freight company then we have other means of transporting goods. We have multiple trucks available if one were to break down during an order. Our maximum allowable time to be down in shipping would be an estimated. The company's growth in the last 5 years has been a substantial growth by the year 2005the company has shipped an estimated 19 million copies.



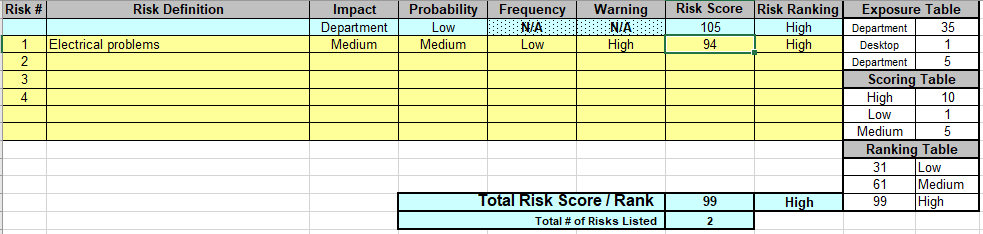
**Manufacturing department:**

Our manufacturing department is a vital part of our business, we are losing money every second it is offline. Therefore making our manufacturing department mission critical. We have different plans of action depending on the situation. If a power outage hit the building we should have backup generators and UPS (uninterruptible power supplies) working to keep our manufacturing department powered until we can safely turn off the machinery. If we are looking for a sustainable option we should use batteries and solar panels to keep our department going, this is stated again further into the document (See Power Outage for more information). If a machine malfunctions or completely breaks down we should have spare machines to replace the problem. Once the machine is fixed it can be put into storage until another machine malfunctions. This allows us to swap and fix machines quickly with minimum downtime.



**Running electricity:**

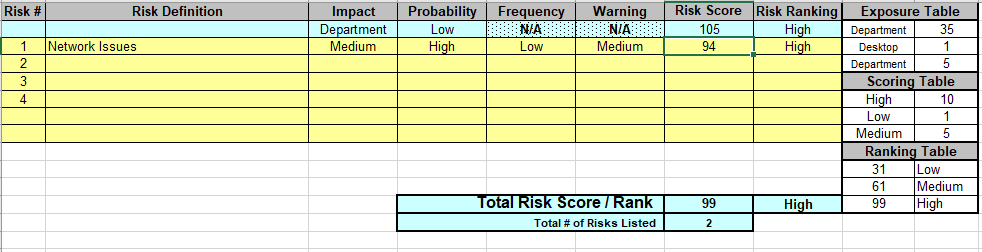
Maintaining electricity throughout the building is an important part of any infrastructure. To deal with electrical problems we are in favor of adding generators and UPS’ (uninterruptible power supply), for small unexpected outages, and solar panels connected to batteries for prolonged outages (See Power Outage for more information). This should give us enough time to safely power down equipment, devices, machinery, etc. We also hope to keep devices and equipment safe from electrical surges through surge protectors and UPS’. Electrical problems are an important problem that will eventually affect our infrastructure, keeping our infrastructure ready and safe will keep us from losing money.



## Important:

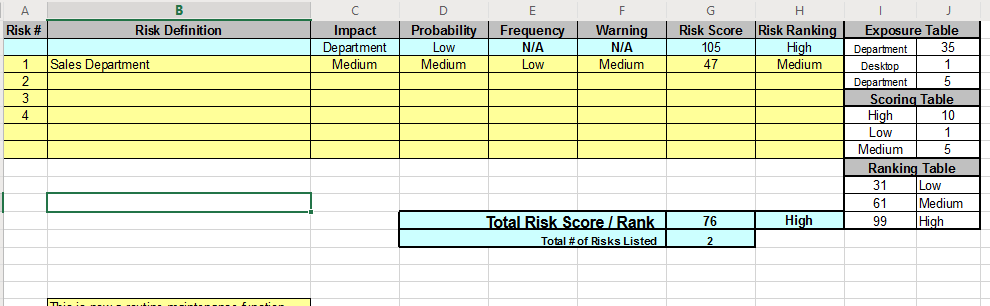
**Running network:**

Our network must always be kept safe and online. Keeping servers online and protected through UPS’ and up-to-date security devices and software. DDoS attacks could disable our networks and malware/ransomware attacks can render our devices useless and could compromise client data. The best way to mitigate this risk is to keep our employees trained and aware of network threats, keep firewalls and other security devices/software updated, and creating “honeypots”(fake servers and/or networks) to help keep our main network safe.As stated before, we will be using UPS’ and generators to keep our servers and clients online while we safely shut them down. Surge protectors will also be used to prevent any unnecessary electrical problems that could cost us thousands in repairs. Keeping a cluster of servers that can replace each other is important. If one server goes offline, we can depend on the other servers to take its job and continue to offer the data/services the malfunctioning server was offering. We can then fix the server or replace it, keeping our network online with little to no downtime.



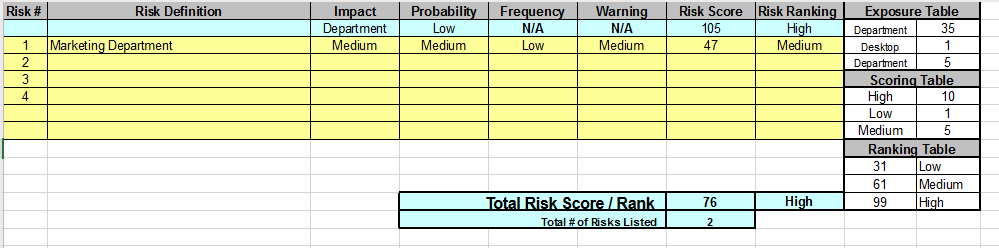
**Sales department:**

The sales department works in unison with the shipping department. They ensure our orders are being sold and that deliveries will be prompt and on schedule. The sales department works in unison with the shipping department as they sell the product and inform the shipping department where the products will be shipped to. If the sales department would go down we would be able to outsource the information to another building to help us with the shipping department.



**Marketing department:**

The marketing department is in charge of finding publisher contacts. They have provided the company with various names including but no limited to: Nintendo, Midway, Capcom.Activision, and Electronic Arts. Without the marketing departments hard work the company would have not been successful. Marketing also helps with getting our name out there this way companies out there know what Digiknights is all about. THe company focuses on making games and fulfilling orders on time. Now that the company has been established the marketing department can afford some down time. Therefore the marketing department is important but not mission critical.



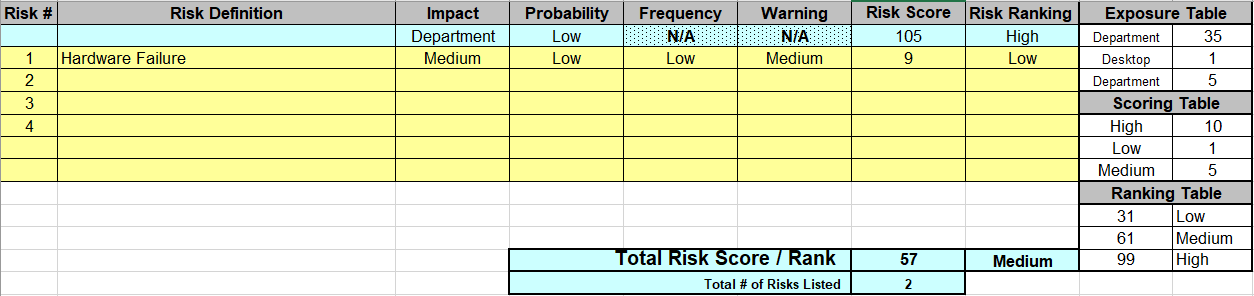
## Minor:

* Research and development team (improving production system)
* Administration for each mission-critical function (non-IT)

## Mission Critical Functions (Non-IT):

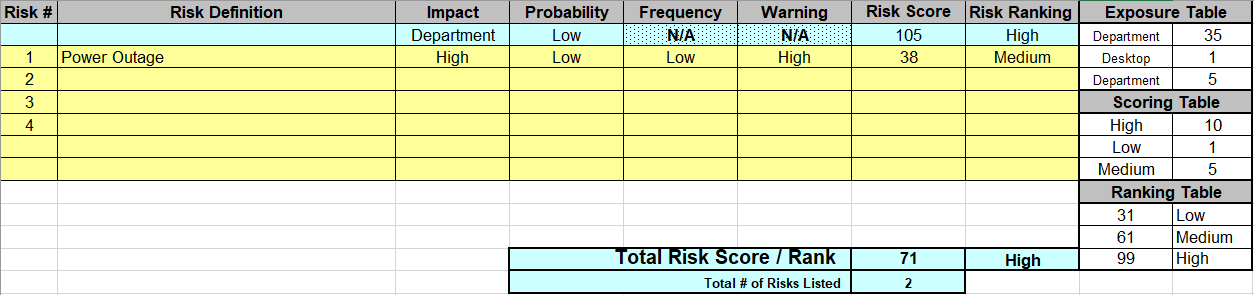
**Hardware Failure:**

Sometimes machines that make workflow in production fail or crash. These machines can often be really expensive to repair or replace. But in the end it is still cheaper for a business to use machines if they can instead of people because there is less room for mistakes and when a machine fails, it can either be repaired or replaced. Hardware failure doesn’t just have to mean automated machines that make production easier, it can also mean hardware tools that are essential for creating products like saws, forklifts, disc printers, etc. can cost the company a lot of money to repair or replace depending on the type of hardware that breaks. Since this company will need a lot of hardware to mass produce discs, the risk of at least one machine failing is only going up.



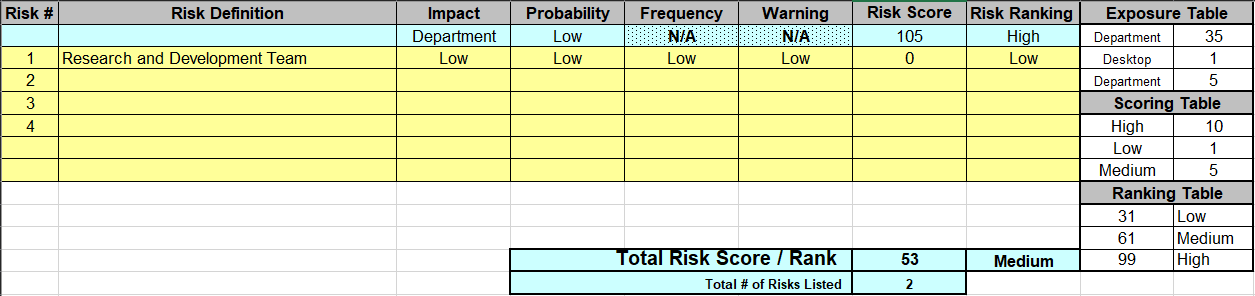
**Power Outage:**

If the power goes out to the office building it can seriously disrupt the work progress of the company. Whether the power goes out for 30 minutes or a couple of days, it will still disrupt the amount of work that is going to get done. The longer the power is out the worse it is for the company. Having battery backups is really important because it can let everything in the office continue running until the power from the city grid comes back online. Having solar panels on top of the building and having that excess power being stored in battery pack is one of the best ways to prevent the office building from going completely offline.



**Research and Development Team:**

The research and development team is extremely important for the future of any business. If a business is not constantly innovating in its industry, it will fall behind its competitors and be run out of business. If the research and development team temporarily shuts down it doesn’t cause a lot of damage but if it is shut down or not innovating for a long time, it can have a large negative impact on the company. It is mission-critical because without it, the company will eventually run out of business. This team doesn’t need a lot of the company’s resources put into it, it just needs to have a lot of talented people constantly thinking of new ways to improve their product.



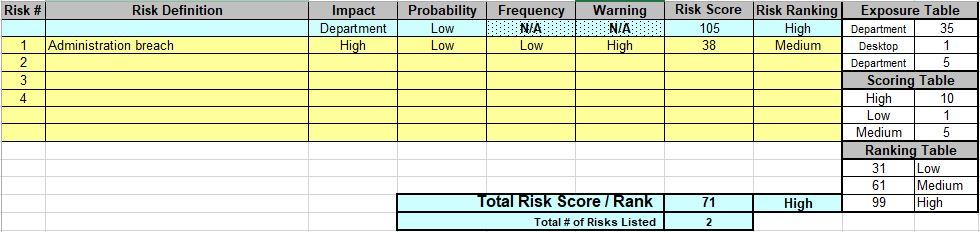
**IT Department**

The IT Department is the backbone which supports the company, they are responsible for any IT related issues that would affect the company even those that are unforeseen and unexpected such as Information data breaches. If the IT department themselves are faced with weak infrastructures and outdated systems then they are potentially vulnerable to attacks that would result in the compromisation of their systems and that of the company in general. An IT department ought to adhere to all standards and policies and also be very well up to date with every equipment and tools used in the response to any technical issue.



**Administration**

Administration is a big part of all of the computers of the entire network. The administration is responsible for major things in the network and can access all things inside the network. If something where to get the password or get into an administrator account the company can be hurt very hard. They can get all of the data that is stored on the servers, from employee data like names to social security numbers. They could get sales numbers and users credit card numbers and debit card numbers and info. This can stop everything in progress and put everything that is currently being worked on halt until the problem is resolved.



# Section III: Backups

### A. Backup and Restore Sections

1. What data would be backed up
2. What data would be backed up to
3. Software used for the backup
4. Would the backup be incremental, full, or both
5. How long would the backup take based on the method of replication
6. What is a good method of backing up the vCSA appliances
7. Cost of Cloud vs On-Premise

### What data would be backed up:

**High Priority:**

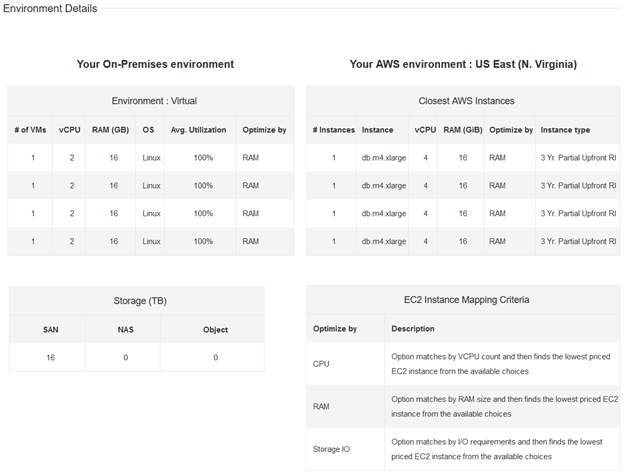
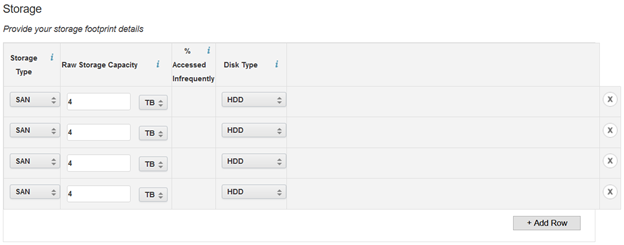
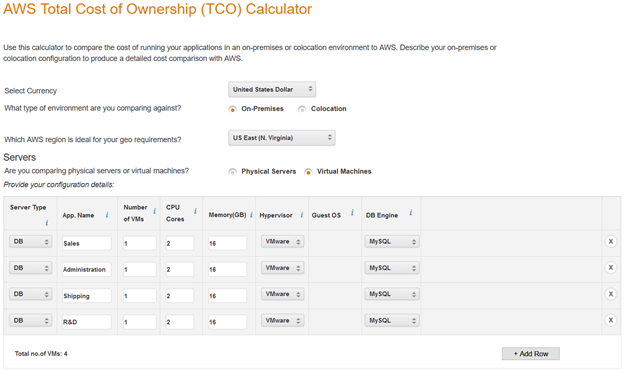
1. Sales information regarding manufacturing, distribution, and destinations of the product. Tracking information should also be reliably stored in a back up to prevent disasters from having a greater financial burden on the company.
2. Information from the administration department containing any financial information regarding the company or it’s employees. All information regarding employees such as contacts, payment information, and other data should be a higher priority for the company to have stored and backed up.
3. Shipping information regarding our contacts, expected arrival dates of supplies, and expected distribution dates should have a higher priority in being backed up, as being unable to locate a necessary shipment could impact reputation along with financial damage.

**Low Priority:**

1. Information from the research and development team have important functions which bring increased margins of profit to the company by researching ways to cut manufacturing expenses. However, the information isn’t crucial to the functions of the company, as such they aren’t a priority in keeping backups of the information.
2. Administration information unrelated to any financing or HR related information (employee information). Examples of information would be training modules and scheduling.
3. Marketing information, while important to the company’s growth with proven results, isn’t a high priority to being backed up. The information from the department isn’t a high priority since the functions and information from the department aren’t crucial or a necessity to the continuity of the company in the event of a disaster.

### What the data would be backed up to:

The data would be backed up to virtual machines on the cloud computing platform, AWS. The storage type would be SAN on HDD to lower expenses. The 16 TB storage databases would be spread across 4 different VMs that have 2 CPU cores and 16 GB of RAM per VM. The VMs will be running MySQL.



### Software used for the backup:

We will be using MySQL on the AWS virtual machines. MySQL has 3 different business oriented editions we can choose from: standard edition, enterprise edition, and cluster edition. We will be using MySQL Enterprise Edition since we are only using 4 VM’s to store information. If we wanted to spend an extra $5000 and get some more features such as cluster management and geo-replication we could go Cluster Edition. MySQL Enterprise edition comes with Transparent Data Encryption, meaning all of our data will be encrypted while at rest and decrypted when read. It also allows us to create full, incremental, and partial backups. MySQL Enterprise edition comes with a firewall that blocks SQL injection attacks through whitelisting. It also has intrusion detection, real time monitoring, and can block suspicious traffic. Overall, MySQL Enterprise edition is a great way to store our data backups since it offers quick deployment, security, and easy management.

### Would the backup be incremental or full or both:

A combination of backup types will be used to ensure quick and reliable recovery. Across all information being backed up, periodic full backups will be created with a monthly schedule. Using the created full back ups, differential backups will be created on a daily basis using the latest full backup as its reference point. Using a differential backup would allow for faster restore times to ensure quicker recovery with the downside of larger storage required and more data being backed with each cycle until the next full backup.

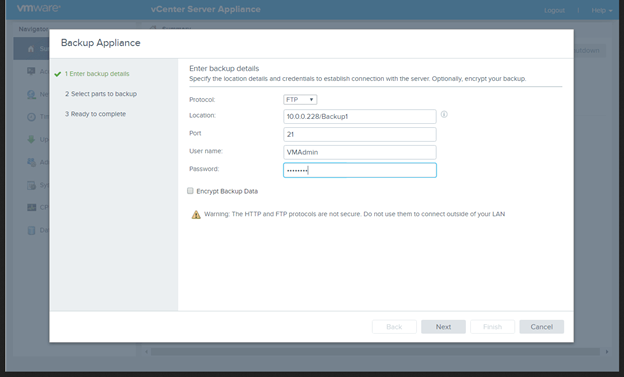
### How long would the backups take based on the method of replication?

The initial backup will take a couple of days depending on the network connection to back up 16 TB of data. Backups would then be conducted once every month to ensure that backups are up to date. If need be, the data could instead be scheduled to be backed up weekly instead of monthly.

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

There is a backup feature within vCenter Server Appliance that allows you to backup your vCSA appliance. It allows you to choose which method you would like to send the backfile as it even allows you to send it as an encrypted file (preferred method) where you can have a key pair and only the person that has the key can open that file.

You must have an FTP, FTPS, HTTP, HTTPS, or SCP server up and running with sufficient disk space to store the backup.



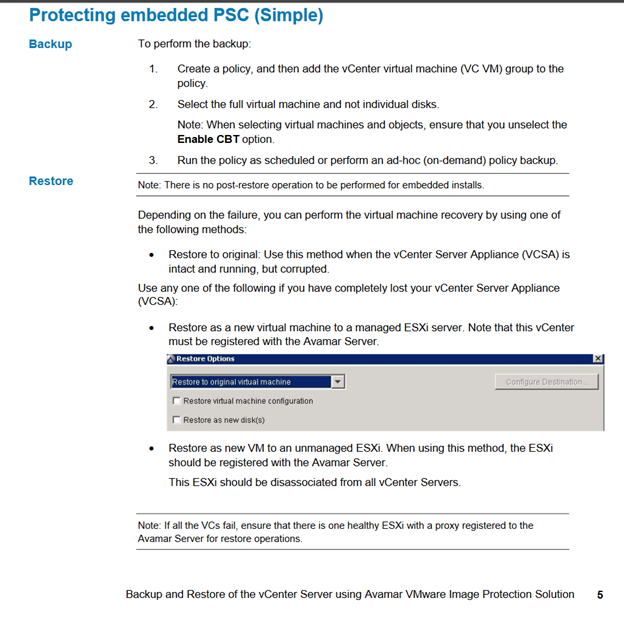
Backup files then save as a a .tar files and in some instances take up to 757 MB in Hard Drive space.

By using the VMware method it is very straight forward. ALso FTP is not recommended unless you are on a secure network in a LAN not open to the public. In any instances FTP and any unencrypted transactions are not recommended.

For the restores to complete successfully, perform one of the following:

● Ensure that these virtual machines use a fully qualified domain name (FQDN) with correct DNS resolution, or

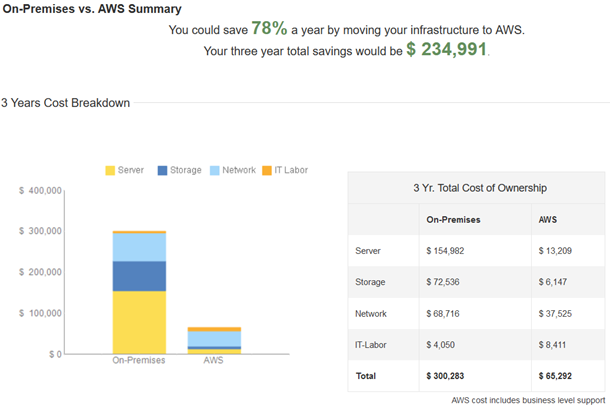
● Ensure that the host name of the machine is configured as an IP address. Note that if the host name is configured as an IP address, the IP address cannot be changed.

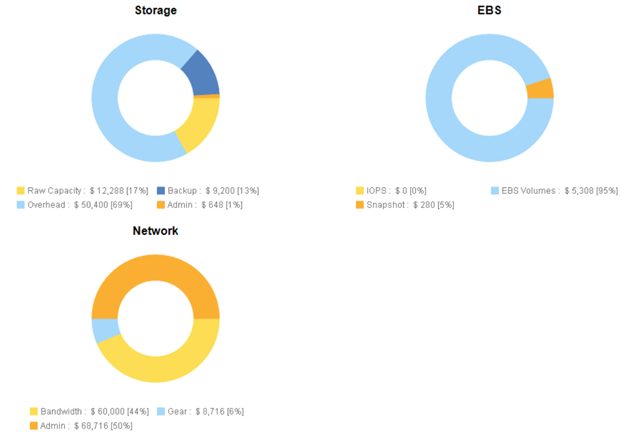
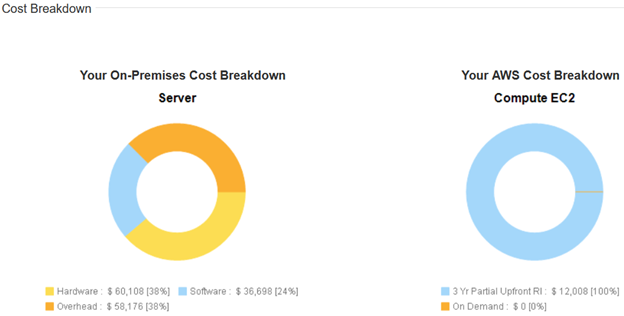


These backup methods are useful in case our systems ever fail . As IT professionals we will be doing constant backups every few minutes or so. It will not slow down production or affect the network at all. Documentation can be provided as needed to help the department install a reliable backup solutions.

### Cost of Cloud vs On-Premise:

Hosting backups on-premise rather than on the cloud can become very expensive. You have to pay for labor costs, hardware of the servers, and repairs if something breaks on the server. Switching to the cloud essentially decreases that cost by a lot. For the 16 TB scenario, DigiKnight could end up saving $234,991 by switching to AWS over 3 years.





### 

# Section IV: Insurance

## Insurance Information

* 1. **Introduction**

With insurance being one of the essentials of a company the company wants to ensure that they are getting the best value for their money. In this document we will discuss some key ideas needed to make the right choice of insurance claims. Some of the keys will be BOPs, workers compensation, and cyber. These are some insurance policies that may one day save your company. As workers compensation covers the most important resource of the company, the employee.

* + 1. **Employee Insurance**

Workers compensation insurance can go a long way when dealing with accidents and disasters that may hurt our employees. Workers compensation insurance will cover accidents in the workplace such as strains, trips, falls, and accidental deaths (Sengupta, Baldwin, & Reno, 2014). We hope to be able to avoid any lawsuits and other health costs by acquiring this insurance. As a company staffed with 48 employees, we hope to be able to cover any expenses caused by unsafe working conditions and avoid legal problems and costs. The cost for workers compensation insurance is $1.85 per $100 in wages in the state of California. There are 3 types of programs we can choose from; state -run program, insurance company, or self-insured. State-run is administered by the state’s department of labor and the employer pays the premiums. Insurance companies also offer workers compensation insurance, which is paid by the employer and the insurance company is in charge of benefits. Self-Insured is only available to companies that are large enough to cover their employees expenses, but they will sometimes use a third-party company to administer claims.

* + 1. **Building Insurance**

Property insurance will cover property expenses caused by natural disasters, theft, and vandalism. An earthquake policy will need to be added to our plan considering we are in an area that is susceptible to earthquakes. Property insurance will cover property costs, computers, equipment, exterior signs, fences, important documents and inventory. Small business owners pay around $500 per year and major corporations pay around $500,000 (howmuch.net). The average business pays $1,000 and $3,00 per million dollars of coverage (howmuch.net). With property insurance we hope to mitigate expenses caused by “Acts of God” or disasters caused by nature, which are unpreventable. We hope to protect all three of our buildings and keep our inventory insured through property insurance.

* + 1. **Insuring Our Machinery**

Having insurance on machine that helps with production of DigiKnight’s product is really important. It can be very costly to replace everything if a machine breaks, depending on the company and what machine they use. Machinery can cost anywhere from $1,000 to $1,000,000 to replace or possible more. Having insurance to help pay for this or pay for it completely will save DigiKnight a lot of money. This company would want to have enough insurance to cover the costs of replacing machine that could break in the future and the average cost of a $1 million policy costs less than $1,000 per year. If more insurance coverage was needed, the average cost of $2 million is around $1,300 per year. So it really isn’t a huge amount of money this company will lose if it has a high insurance coverage plan.

* + 1. **Insuring our IT Infrastructure**

The average cost of IT insurance is anywhere between $650 to $1,300 per year. It really depends on how much a company wants to cover whether that just by critical servers or all IT related systems. Based on DigiKnight’s IT department specifications, you will not want insurance on the basic computers that each department has like the Sales or Administrative department because those are relatively cheap compared to other department’s systems. The 10 servers and the IT department that DigiKnight has will be covered under the IT insurance because those are critical to helping keep the business alive.

## FEMA Continuity Guidelines

According to FEMA’s federal continuity guidelines, there are a few key points to having an efficient continuity plan. Establishing a scope by planning objectives for the company’s continuity plan is the first step in developing a functioning plan. Essential functions are to be identified and prioritized as the foundation of the continuity plan. Alongside critical functions, communications and information systems are a high priority across all locations, primary and alternate. Alternate locations are to be established in order to resume or continue any essential functions. After establishing procedures to protect critical functions it is necessary to test the plan and different solutions to potential problems before an emergency happens to ensure continuity.

# Section V: Backup Sites & Active Disaster Procedures

### A. Activate Alternate Work Sites

**Overview:**

In case of an emergency natural or man made there will be alternate sites available. This will reduce down time and by having these sites ready we can move personnel accordingly with little to no loss of time. There are several events that can happen that will disrupt the business this is why it is essential to have cold and warm sites, A plan has been implemented for each of the events that may occur. These plans will be activated accordingly, The following tasks will take place to activate an alternate site:

* Management team will conduct with Emergency Response Team to assess the damages of the building. The Emergency Response Team will be in charge of ensuring the business is safe enough to access to gather vital records and other important elements( e.g. machinery)..
* Depending on what is able to be retrieved. Transportation will be arranged to transport the vital records and important elements.
* Management and key personnel will travel to site in order to get the sites up and running

.

* Once the site has been activated and inspected other personnel will be allowed on these sites.
* Conduct business as usual and contact Emergency Response Team in case of emergency.

**Contact info:** To notify the use of the new alternate worksite in the event that the main worksite is down all the employees will have given a phone number that they can use and be ready for a site move. A personal email and work email will receive a notice and reasons that the work site is down and where the new work site is.

### B. Alternate Work Site Plan:

**Location:** The location of the alternative site is in Houston, Texas

**Personnel:** Stand by personnel will activate the alternate work site and prep it for use when an emergency happens. This is to make sure that work can continue as normal and be set up for employees to arrive on site. Servers will be active.

**Phone Numbers:** The phone numbers of the employees will be given to the company and will get a phone call and text to let them know that an event has happened and notified that an alternate worksite is now active.

**Managamement:** Management will be the first on site at the alternative site. They need to be there first because they need to understand what resources need to be invested into the different sites and what needs to be done to get the sites up and running if something goes wrong at the main facility.

**BC/DR Team:** A plan to ensure that the company can still continue to run and profit will be made and implemented. This group can be on or off alternative site. As to make adjustments to the plan to have the company still up and running.

**Crisis management:** In the event of a main site going down, the alternate worksite will become the current active worksite to insure the continuation of work and the online presence, to have work and the online transactions will still be active and working. Until the main worksite is fixed and ready to be used as a main work site again.

**Human Resources:** If the main facility does go down, Human Resources are essential in keeping the business alive. They essentially keep track of employees, if some people need to be hired to work at the different sites, Human Resources would be in charge of hiring those employees and making sure they get paid to work at the different sites.

### C. Cold Site Plan:

**Location:** The location for the cold site will be in Arlington, Virginia.

**What equipment is needed:**

In a cold site, most equipment must either be purchased or shipped to the new location, for this reason only a minimal amount of supplies and equipment will be stored in the location before a disaster occurs. Due to the size, expense, and time to order and configure the production machines, the cost of having them already on a cold site is worth the amount of time and potential profits saved in the case of disaster recovery. A small number of desks should already be in place for any machinery, equipment, and staff that arrive earlier than others.

**What resources are needed:**

Due to having minimal equipment and resources being required at the alternative location in a cold site, there is a need for production machinery to be established before the case of a disaster on sight. Apart from the machinery, staff members that can transition to this new site who are trained in creating the foundation of the site and its functions are required alongside a way to transport or purchase any machinery used at the old location. There should be a minimum of a few people per department who can always transition from the current location to the cold site. Senior positions would be preferred for the transition. Backups of the live site should be made on a frequent basis and stored in secure locations for the case of needing to move the company to the cold site.

**Summary:**

A cold site by definition is a location that is a backup site in the event of a disruptive operational disaster at the normal business site. A cold site does not always have the necessary equipment to resume operations immediately. A cold site is less expensive than a warm or hot site but that is because not all the equipment is there or set up so it will take longer for a business to use the cold site to get their business back online and functioning. The pros to having a cold site is that a cold site is not as expensive to set up compared to a warm or hot site. The cons to having a cold site is that **t**he cold site is not ready to be switched over as the main operating facility because not all the necessary equipment is there or even set up. Overall, it is always good to have redundancies so having a cold site is always recommended for businesses that can afford it. Cold sites can also just be used as storage for excess supplies or machinery. You also don’t want to have other backup sites too close to the main site because if something happens like a power outage that can affect a large area, and the cold site is close to the main site, the cold site will most likely also be affected by the power outage. So having the backup sites spread across the state or the country is always a good plan in case something goes wrong that affects a large area, it won’t affect the other sites.

### D. Warm Site Plan:

**Location:** Our warm site location would be Dallas, Texas.

**What equipment is needed:**

Equipment needed for warm site back plan can be inclusive of equipment which includes:

* Available Conference rooms to meet in the case of disaster recovery.
* Areas to change clothes if needed.
* Access to communications services
* Phones, fax machines and copiers.
* Available access to Food and beverages.

**What resources are needed:**

A back up plan for a warm site which otherwise can be described as a bridge between both cold and warm site would normally consist of every possible portion of required hardware, software, data circuits, and other resources needed to quickly restore normal business operations. Also the equipment is expected to be preconfigured and primed to run appropriate applications to support the organization’s operations.

**Summary:**

Warm sites are intended to be a middle ground between cold and hot sites. A warm site is supposed to contain most of the technology infrastructure that a business is needed to run. Servers, clients, and other devices should have software installed onto them and should be ready to use at any moment. We should also have our production infrastructure read to go, since it is a mission critical department. Although we have the network infrastructure running, it does not mean we need to have data available in it. The network infrastructure is supposed to be as good or better than we currently have on our main site. A warm site needs to be far enough away to avoid any disasters that hit the main site and should not be on the same power grid as the main site. We would need to keep our back-ups offsite and/or use a cloud service to handle our back-ups, because main site data is not available on the warm site and losing main site data would delay our recovery time. The price of a warm site surpasses the cost of a cold site, running from $15,000 to $350,000+ depending on the amount of equipment you want readily available. That being said, warm sites are a great way to have mission critical departments ready to go without worrying about smaller departments and they are the middle ground between hot and cold sites.

### E. Hot Site Plan:

**Location:** Our hot site location would be Austin, Texas.

**What equipment is needed:**

Equipment needed for a hot site backup plan would mostly consist of items such as servers, conference rooms for your disaster recovery staff to meet, areas to change clothes if needed, food and beverages available, and possibly even a store to buy clothing, and an exercise area.

**Summary:**

For hot sites, it essentially a replica of the main site. Almost all of the equipment is the same with both of the 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.

### F. Mobile Site Plan:

**Location:** Our mobile site would be located in Seattle, Washington.

**What equipment is needed:**

Since mobile site is a mesh-up of both warm and cold site backup plan, the equipment that would be in the need here could consist of items such as lighting, fax machines, phones, copiers, preconfigured work areas with furniture. Access to communications services would be needed.

**Summary:**

A mobile site backup is a site is pretty similar to warm sites. The difference between the two is that the mobile site’s job is to ensure connectivity in case something goes wrong. It is not meant to be a main facility where all operations can be switched to, it is more of a site that is just used for online connection and services. The facility itself will mainly have the equipment in it but it have as much equipment compared to a warm or hot site. A mobile backup site is less expensive than a hot site and warm site because it just meant for connectivity and services. A mobile site is easy to set up because it only needs to worry about having connectivity and services up. The pros of having a mobile site is that it is less expensive than a warm or hot site. The cons to it is that it only does 2 services. Businesses don’t have to prioritize having a mobile site back up unless they want to and they can afford it. Having a hot and warm site are the best options for backups for a business and a mobile backup isn’t necessary.

### G. Mirrored Site Plan:

**Location:** Our mirrored site location would be Twin Falls, Idaho.

**What equipment is needed:**

The equipment needed to run a mirrored site is the same equipment we would use at the main site. This will be servers, machinery, office supplies, etc. We would also need to find a way to mirror the data we are receiving at our main site and implement it into the mirrored site’s storage. An option is to use Windows Server Active Directory to cluster the servers and mirror the information to the site.

**Summary:**

A mirrored site would require us to create a copy of the main site with exactly the same infrastructure. This would include all of the data being processed in the main site as well. This can also be considered a hot site considering how much infrastructure is being added to the site. A mirrored site is based on the same principles that make up a hot site. The most important thing about a mirrored site is having the servers processing and storing the same data the main site servers are receiving/creating. Maintaining a mirror site is as expensive as maintaining a hot site, since you are using the same resources in both. Although quickly available after a disaster, any data that was being mirrored to the site during the disaster will be lost. Data corruption is a big worry when running a mirrored system. We want to make sure none of the data is being corrupted at any point, if it does, it could lead to major losses and delays during a real emergency.

### H. Active Disaster Procedures

**Crisis Communication Command Center:**

**Location:**

The crisis communication command center will be located at the main office, while contact lists are also going to be located across all other sites implemented to ensure proper communication in the event of a crisis. 2725 E. Technology Ave, Freemont, CA 94536

**Personnel & Phone Numbers:**

|  |  |
| --- | --- |
| Main Site Phone Number | 415-555-2668 |
| CEO (Carlton Smith) | 415-555-7841 |
| Head of Administrator (Mark Saunders) | 415-555-8643  415-555-0180 |
| Head of Sales (Diana Ford) | 415-555-6312  415-555-0200 |
| Head of Manufacturing (Linda Kraemer) | 415-555-6161  415-555-0150 |
| Head of Research & Development (Carlton Bowden) | 415-555-3223  415-555-0100 |
| Head of Maintenance (Michael Winters) | 415-555-3970  415-555-0400 |
| Head of Advertising (Michael Churchill) | 415-555-3131  415-555-0160 |
| Head of Shipping (Kenneth Gilliam) | 415-555-6431  415-555-0130 |
| Head of Purchasing (Katherine Cavenaugh) | 415-555-3298  415-555-0120 |
| Head of Security (Brett Kelcey) | 415-555-3852  415-555-0170 |
| Head of IT (Alicia McKellips) | 415-555-8352  415-555-0190 |

**Notify Crisis Communication Command Center:**

Will contact the appropriate personnel including management, BC/DR team, crisis management team, and HR. There will be triggers that will influence the decision making on when it is appropriate to communicate crisis team:

1. If a disruption appears to be intermediate on initial assessment, within 2 hours:

• Attempt to gather information from the emergency responders, if appropriate.

• Activate the damage assessment team.

• Notify the CMT to be on standby notice.

2. After 2 hours from event notification, gather initial evaluation from damage assessment team. Analyze data and determine:

• Take remedial action and resolve issues.

• Partial or full activation of BC/DR plan.

3. After 3 hours, notify CMT of next steps (stand down, fully activate).

source(Snedaker, 2011)

**Executive Plan:**

Once a disaster hits, all of our teams are responsible for completing their assigned tasks.

**Employees:**

Employees are responsible for reporting any incoming/ongoing disasters that may affect the main site. During a disaster, employees are expected to follow the emergency policies set by HR and Management.

**Management:**

Management must report on the disaster and contact the BC/DR team, crisis management team, and emergency services if needed. Management must contact HR and make sure employees are leaving the facility safely and/or following the emergency policies set by HR. Management knows how important it is to quickly contact these groups to avoid major losses, that being monetary and human life.

**BC/DR Team & Crisis Management Team:**

The BC/DR team is responsible for recovering any off site back-ups and contacting any sites that are ready to be moved into. Our hot site and/or mirrored site is the first to be contacted. The next option, if the first two are not available, is our warm site and/or mobile site. If we do not possess the previous options, we will contact our cold site. DigiKnight will always have at least 2 site options available (apart from the main site). Different procedures will have to be followed depending on the type of site we possess. Our CM team is responsible for contacting our clients and resolve any problems that may come up. It is also responsible for managing shipping routes that will be affected by the disaster and the CM team will contact retail stores that will be affected as well.

**Important Documents:**

Immediate things that need to be done is to secure important documents. Important records that need to be kept track of are:

● Service Contracts (Computers)

● Service Contracts (Machines)

● Service Contracts (Software)

● Service Contracts (Office Equipment – Copies, Etc.)

● Sales Receipts (Records of Store Distribution)

● Distribution Contracts W/ Publishers (Legally Allows Production)

● Building Blueprints

● Machine Blueprints and Manuals

● Employee Hiring Records (Drug Test Results, Applications)

● Corporate Handbook

● Corporate Phonebook

● Local Phonebook

● Supply Purchase Receipts

● Advertising Prints

● Company Authorized Photos

● Customer Lists

● OSHA Compliance Data

● EPA Information

● Accounting Files

● Tax Records

● Computer Manuals (from the manufacturer)

Since there are only hard copies of these documents so far, a backup to the cloud will be conducted immediately to ensure that they are kept safe and available at all times. Once the initial backup is complete, a scheduled backup process to keep the documents up to date will be conducted once a week. These are the most important documents that need to be tracked and have backups to ensure their integrity.

**Hot site & Mirrored Site Procedure:**

Hot sites and Mirrored sites are already available and need minimal set up. The BC/DR team is responsible for making sure everything is in working order and ready to be used as soon as possible. All data must be present in the IT infrastructure and must be as close to up to date as possible. The team is responsible for salvaging any corrupted data and hardware. Management should be contacted once the site is officially ready to be used.

**Warm site & Mobile Site Procedure:**

Warm sites and Mobiles sites are halfway between cold and hot, they will require some more setup and maintenance. BC/DR is responsible for setting up mobile sites and/or writing down everything that is missing in our warm site. Since warm sites should have IT infrastructure already, the BC/DR team is responsible for making sure all systems are healthy and ready. They are also responsible for updating the systems and starting the data recovery process from our back-ups. Management should be contacted and notified about missing machinery and/or any other crucial items that may need to be bought.

**Cold Site Procedure:**

Cold sites are the slowest to set up due to them usually not having any hardware and equipment available. The BC/DR team is expected to write down everything crucial that needs to be bought to get the business back up and running again. The first items ordered must be mission critical and should be enough to bring back production and IT infrastructure. BC/DR is responsible for maintaining contact with management, letting them know about any problems, suggestions, and updates.

# 

# Section VI: Emergency Contacts & Event Templates

### Emergency Contact Information & Procedure

|  |  |
| --- | --- |
| FremFIrst ont Fire Department/Stations | (510) 494-4200  911 |
| Fremont Police | Police Department (Non-Emergency): (510) 790-6800  Call or text 911 |
| Hazardous materials | Fremont Recycling & Transfer Station: 41149 Boyce Rd, Fremont, CA 94548 (510) 252-0500    Alameda County Household Hazardous Waste: 41149 Boyce Rd, Fremont CA, 94538 (800) 606-6606 |
| Hospitals | Washington Hospital: 2000 Mowry Ave, Fremont, CA 94538 (510) 797-1111  Emergency Room #: (510) 791-3430    Kaiser Permanente Emergency Room: 39400 Paseo Padre Pkwy, Fremont, CA 94538 (510) 248-3000 |

For all life threatening scenarios, 911 is the best method of contact emergency services. In the event of an emergency where employees can’t call, texting 911 is also an option in Fremont, CA. When texting, provide an address, cross streets, and landmarks when possible along with what type of emergency is happening. A dispatcher will communicate through text in order to get more information, so keep the phone available. Texts can only be received in English, doesn’t accept any slang or abbreviations, can’t receive images or video, have a 140 character limit, and can only be sent to 911 (no other contacts can be attached to the texts). If there is no response from a dispatcher, contact 911 through a different device or by calling. The police can also be contacted through a non-emergency line for non-life threatening situations. If for any reason an employee is unsure if something qualifies as an emergency, they should contact through the emergency line.

### Event Templates

**Event Report Template:**

**Event Overview:**

● **Date:** Add detail here.

● **Venue:** Add detail here.

● **Speakers:** Add detail here.

● **Ticket Price:** Add detail here.

**Purpose:**

The purpose of this event was to…

**Measures of Success:**

|  |  |
| --- | --- |
| **Measure** | **Actual** |
|  |  |
|  |  |
|  |  |

**Achievements**

● Achievement #1.

● Achievement #2.

● Achievement #3.

**Recommendations**

● Recommendation #1.

● Recommendation #2.

● Recommendation #3.

**Budget**

|  |  |
| --- | --- |
| Budgeted Income | $ |
| Budgeted Expenses | $ |
| Actual Income | $ |
| Actual Expenses | $ |

**Budget Commentary**

● Budget note #1.

● Budget note #2.

● Budget note #3.

**Logistics**

**Observations and Recommendations**

● Add detail here.

● Add detail here.

● Add detail here.

**Feedback**

**Feedback Form**

● The feedback form was emailed to X delegates.Y delegates completed the survey.

● Interpret Information and record on form.

**Log Template:**

Activation Log

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Date | Work Task | Hours | Notes | |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Damage Assessment & Checklist Templates:**

**Structural damage:**

|  |  |  |
| --- | --- | --- |
| Step | Action | Deliverable |
| 1 | Check support structure for building | Inspectors/Engineers will be in charge of determining the structural integrity of the building. |
| 2 | Find any damage to wall/floor | Inspectors/Employees will inspect the building for any damage. |

**Health and Safety:**

|  |  |  |
| --- | --- | --- |
| Step | Action | Deliverable |
| 1 | Check-in with all employees | Employees are to be accounted for and we must make sure they are in a safe area. |
| 2 | Find any injured employees | Seek injured employees and call emergency services if needed. |
| 3 | Work with emergency services | Assess employee injuries and casualties with emergency services. |

**Risks Template:**

|  |  |  |
| --- | --- | --- |
| Step | Action | Deliverable |
| 1 | Identify hazards and their potential for causing harm. | An inventory of hazards. |
| 2 | Rank hazards by priority. | This list will be useful in planning further action. |
| 3 | Determine hazard elimination or risk control measures. | A record of hazard elimination or risk control measures at various locations.  Adequacy of hazard elimination or risk control measures.  A list of controls required or recommended by legislation, standards, best practices, or organizational policies. |
| 4 | Eliminate the hazard, or implement risk controls. | Controls are in place and functioning appropriately. |
| 5 | Measure the effectiveness of controls. | Monitor periodically to confirm controls continue to function. |
| 6 | Make changes to improve continuously. | Monitor for improvements. |

## 

**Disaster Recovery Service Contact:**

|  |  |
| --- | --- |
| **Items to include in procedures for contacting disaster recovery service providers** | **Status (e.g, Completed, Pending, or N/A)** |
| **Names and titles of employees who are authorized to contact the disaster recovery service providers** |  |
| **Contact information and locations of disaster recovery service providers** |  |
| **How to describe needs to these service providers** |  |
| **How facilities and locations should be identified for these service providers** |  |
| **Information on negotiated contacts with these service providers** |  |
| **Information on paying these service providers if there are no negotiated contracts** |  |
| **How to access emergency funds to pay disaster recovery service providers** |  |

**Contacting Stockholders and Investors:**

|  |  |
| --- | --- |
| **Items to include in procedures for working with stockholders and investors** | **Status (e.g, Completed, Pending, or N/A)** |
| **Name and titles of employees who are authorized to talk with stockholders and investors** |  |
| **A list of executives assigned to stockholder and investor relations** |  |
| **Contact information and locations of large stockholders and investors** |  |
| **How to establish a stockholder and investor relations area at the emergency operations center** |  |
| **A process to update stockholders and investors on the status of disaster recovery efforts** |  |
| **A process to provide stockholders and investors with a final report when recovery is complete** |  |

**Contacting Suppliers and Service Providers:**

|  |  |
| --- | --- |
| **Items to include in procedures for working with suppliers and service providers** | **Status (e.g, Completed, Pending, or N/A)** |
| **Names and titles of employees who are authorized to work with suppliers and service providers** |  |
| **Contact information and locations of suppliers and service providers** |  |
| **How product lines or services should be identified when contacting suppliers and service providers** |  |
| **What to tell suppliers and service providers about disasters** |  |
| **What to tell them about recovery of operations** |  |
| **What suppliers and service providers should do if they need to contact the organization during the disaster** |  |

**Contacting Customers:**

|  |  |
| --- | --- |
| **Items to include in procedures for working with customers** | **Status (e.g, Completed, Pending, or N/A)** |
| **Names and titles of employees who are authorized to work with customers** |  |
| **Contact information and locations of key customers** |  |
| **How product lines or services should be identified when contacting customers** |  |
| **What customers should be told about disasters** |  |
| **What they should be told about recovery of operations** |  |
| **What customers should do if they need to contact the organization during the disaster** |  |

# Section VII: Testing Procedures

### Alarms

One alarm should be installed in each room, two to four alarms in hallways and large rooms. Fire alarms need to be visually inspected once a week. This means we should check the alarms LED’s, fuses, power supply, etc. We need to check the alarm’s power supply every 6 months, especially if the alarm runs on batteries. Corrosion can cause the alarm to malfunction and dead batteries renders the alarm useless. We will test the fire alarm system every 6 to 12 months with the help of the local fire department or a private company. We will activate the alarms to make sure they are functioning properly. If the alarm runs on batteries, we will make sure to change them out during this test.

### First Aid Supplies and CPR

We should have at least four first aid kit stations around our facilities. One in each building and an extra inside the manufacturing facility. Gloves and face masks will be available for our manufacturing employees. They will be readily available to anyone. We will also have four Automated External Defibrillators(AED). The International Safety Equipment Association created a standard on what needs to be included in the first aid supplies. Some of the items we will include are:

○ First aid guide

○ AED

○ Bandages and tape

○ Antiseptic and Antibiotic treatment

○ Burn treatment

○ Gloves and face masks

○ Cold pack

○ Eye/Skin wash

○ Hand sanitizer

○ Common Medicine

We will be going for class B kits, which will contain a large assortment of supplies. The full list can be found on the ANSI/ISEA Z308.1-2015 document, which is sold by ANSI. These supplies will be checked and/or supplied monthly.We will be refilling the first aid supplies every month.The local emergency service or a private company will be in charge of testing out the AED every 2 to 6 months.

### Fire Suppression Equipment

Our fire suppression system consists of sprinklers and fire extinguishers. We will have 2 fire extinguishers in each building, each one must not exceed the 75 feet travel distance indicated by the NFPA. The NFPA also requires us to place one of the fire extinguishers close to the stairway in our second building. Our sprinklers will be situated alongside our alarms.We will be using a pre-action sprinkler system, which will help us prevent false alarms and will help protect important machinery and computer equipment. The system and equipment will be checked every month with the help of the local fire department or a private company. The sprinkler system can be tested every 6 to 12 months.

# Section VIII: Evacuation Procedure

## Evacuation and Safe Space Plan

Emergency services are to be called immediately. If accessible and if the conditions are safe, employees are expected to evacuate the building and stay outside or leave the premises completely. If available, the sections marked as Assembly points are the prefered areas where employees should go to. If not, employees are to stay inside and stay safe. All rooms are marked in the plan and they contain their appropriate resources. In an earthquake, employees are expected to stay under tables and desks, and they are expected to stay away from the building walls and doorways. If evacuation is not an option and if accessible, the break rooms are the recommended assembly areas. In any other situation or if needed, first aid kits can be found in employee break areas. One can also find food and water in the break room. Radios can be found in the maintenance rooms. If accessible, management and/or maintenance staff is responsible for shutting down utilities. Shut-off for all utilities can be found in the maintenance rooms alongside the sprinkler and fire alarm controls. Think properly through the situation, employees are not expected to save lives. Proper training is done after the hiring process. This training involves a video with questions the employee must answer.

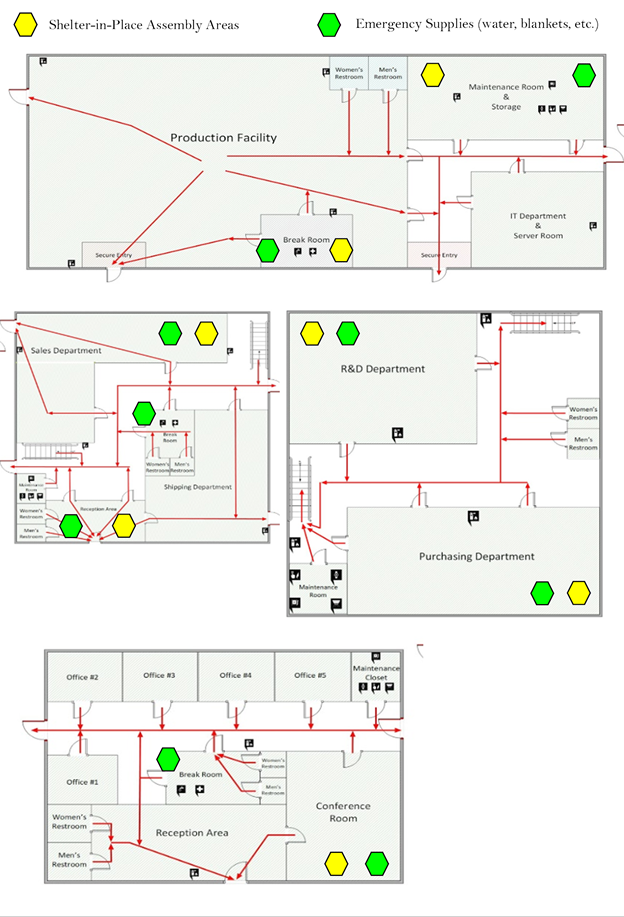
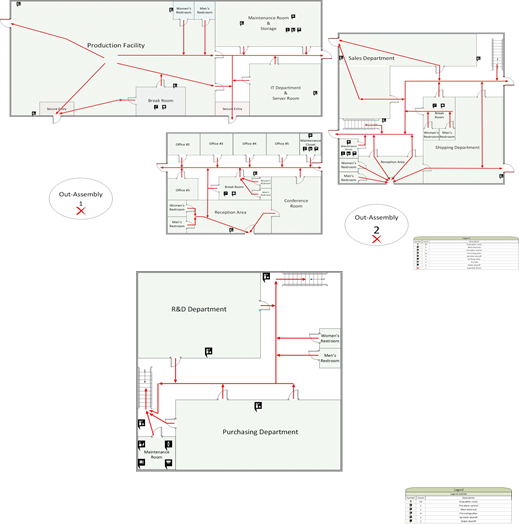
Local Roads that can be used to evacuate:

● Parelta Blvd.

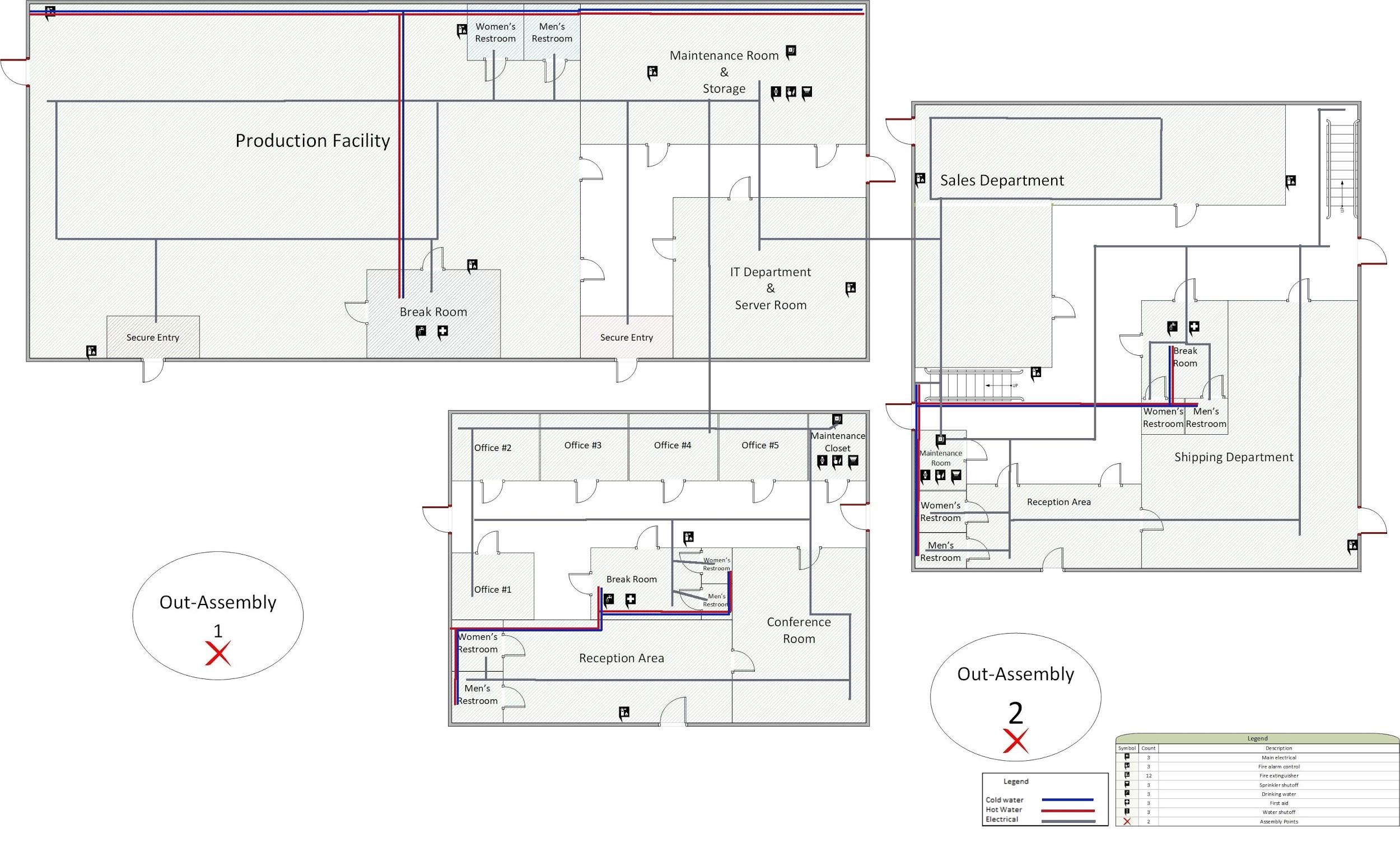
● Mission Blvd.

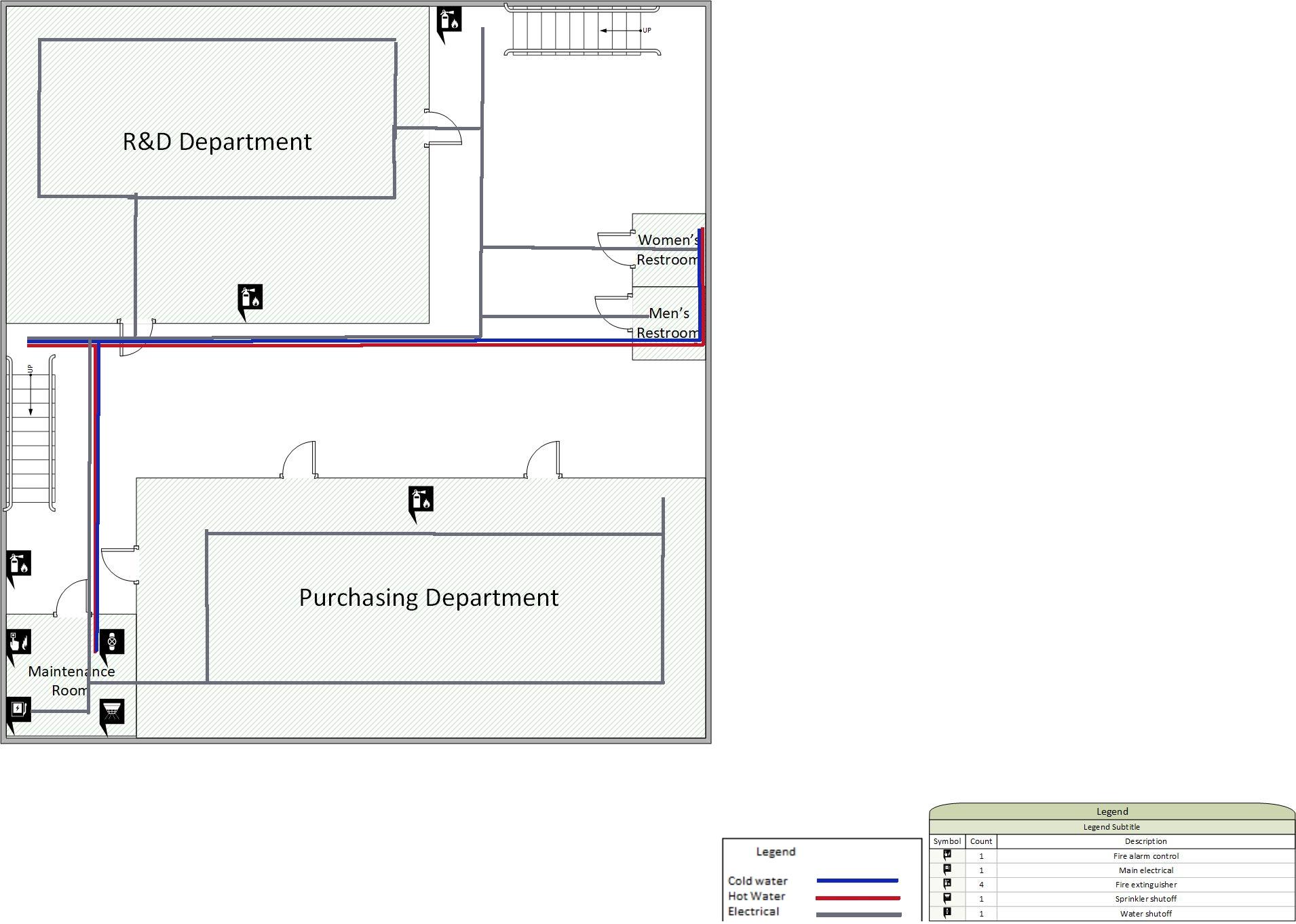
● Niles Blvd.

● Freemont Blvd.

● Mowry Ave.

The location of the water lines and electric line blueprints can be obtained from the building manager or from the county clerk.The building manager will be responsible for documenting any changes done to the building (e.g new installs,added water lines, etc.) Anything done to the building will comply with the state’s building codes and the building manager will be informed immediately of any changes.





References:

ANSI, & ISEA. (2015). ANSI/ISEA Z308.1-2015 - American National Standard û

Minimum Requirements for Workplace First Aid Kits and Supplies. Retrieved from https://webstore.ansi.org/Standards/ISEA/ANSIISEAZ3082015

Ascendtech Inc. (n.d.). List of 6 Common Contributors to Hard Drive Failure. Retrieved from https://www.datarecoverylabs.com/company/resources/hard-drive-failure

AWS Calculator (n.d.) Retrieved July 7, 2019 from https://awstcocalculator.com/

CEA - California Earthquake Risk Map & Faults By County. (n.d.). Retrieved June 1, 2019, from

https://www.earthquakeauthority.com/California-Earthquake-Risk/Faults-By-County

Continuity Resource Toolkit. (n.d.). Retrieved June 16, 2019, from

https://www.fema.gov/continuity-resource-toolkit

CostOwl.com. (2019). 2019 Average Business General Liability Insurance Rates: How Much Does Business General Liability Insurance Cost?. Retrieved from https://www.costowl.com/insurance/insurance-general-liability-cost.html

CostOwl Staff. (n.d.). CostOwl.com. Retrieved June 16, 2019, from https://www.costowl.com/insurance/insurance-general-liability-cost.html

Data backup types explained: Full, incremental, differential and more. (n.d.). Retrieved July 7, 2019, from https://searchdatabackup.techtarget.com/tip/ Data-backup-types-explained-Full-incremental-differential-and-incremental-forever-backup

Emc how to backup vCenter.Retrieved from https://www.emc.com/collateral/white-papers /302-004-537-backup-and-restore-using-avamar-vmware.pdf

Fireline. (2014, December 30). 4 Types of Fire Sprinkler Systems. Retrieved from

https://www.fireline.com/blog/4-types-fire-sprinkler-systems/

Guard, G. (2018, April 24). ANSI First Aid Cabinet Requirements – Green Guard.

Retrieved from https://www.greenguard.com/tag/ansi-first-aid-cabinet-requirements/

Incremental Backup vs. Differential Backup. (n.d.). Retrieved July 7, 2019, from http://hyper-v-backup.backupchain.com/incremental-backup-vs-differential-backup-a-comparison/

Kaspersky Staff. (n.d.). Distributed Denial of Service: Anatomy and Impact of DDoS Attacks. Retrieved June 1, 2019, from https://usa.kaspersky.com/resource -center/preemptive-safety/how-does-ddos-attack-work

Kirvan, P. (2012, January). Hot, warm, cold: What’s the best DR site for your company?.

Retrieved from https://searchdisasterrecovery.techtarget .com/magazineContent/Hot-warm-cold-Whats-the-best-DR-site-for-your-company

Koorsen Fire & Security. (2018, May 4). How Often Does the Fire Alarm Need to Be Inspected?. Retrieved from https://blog.koorsen.com/how-often-does-the-fire-alarm-need-to-be-inspected

Duncan, I. (2019, June 1). Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts. Retrieved from https://www.baltimoresun.com/maryland/baltimore-city /bs-md-ci-ransomware-email-20190529-story.html

Disaster recovery site options. (n.d.). Retrieved from https://searchdisasterrecovery.techtarget.com/tip/Disaster-recovery-site-options

Hamill, V. (2019, April 22). 15 Best Small Business Insurance Companies 2019. Retrieved June 16, 2019, from https://fitsmallbusiness.com/small-business-insurance-companies/

Howmuch.net. (n.d.). Commercial Property Insurance Cost. Retrieved from https://howmuch.net/costs/commercial-property-insurance

Insureon. (n.d.). How Much Does Workers' Compensation Insurance Cost? Retrieved from https://www.insureon.com/small-business-insurance/workers-compensation/cost

Insureon Staff. (n.d.). How Much Does General Liability Insurance Cost? Retrieved June 16, 2019, from https://www.insureon.com/small-business-insurance/general-liability/cost

Kelly, R. (2017, May 7). Almost 90% of Cyber Attacks are Caused by Human Error or Behavior. Retrieved from https://chiefexecutive.net/almost- 90-cyber-attacks-caused-human-error-behavior/

MySQL. (n.d.). MySQL :: MySQL Enterprise Edition. Retrieved from https://www.mysql.com/products/enterprise/

Ncipher. (2019). 2019 Global Encryption Trends Study | Encryption Statistics and Strategies | Ncipher. Retrieved from https://www.ncipher.com/2019/global-encryption-trends-study

NOLO. (2010, November 23). Who Actually Pays for Workers' Compensation?. Retrieved from https://www.disabilitysecrets.com/workmans-comp-question-20.html

Rouse, M., & Crocetti, P. (2018, December). What is warm site? - Definition from WhatIs.com.

Retrieved from https://searchdisasterrecovery.techtarget.com/definition/warm-site

Searchcio Staff. (2010, November). What is hot site and cold site? - Definition from WhatIs.com. Retrieved June 23, 2019, from https://searchcio.techtarget.com/definition/hot-site-and-cold-site

Sengupta, I., Baldwin, M., & Reno, V. (2014, August). REPORT: Workers' Compensation: Benefits, Coverage, and Costs – 2012 Data. Retrieved from http://www.nasi.org/research/2014/report-workers -compensation-benefits-coverage-costs-2012

Shacklett, M. (2017, October 26). Your business might get hacked: Here's how to get insured. Retrieved from https://www.cnet.com/how-to/assessing- cyberinsurance-for-your-business/

Snedaker, S. (2008, January). Business impact analysis for business continuity: Upstream and downstream losses. Retrieved from https://searchitchannel.techtarget.com/feature/ Business-impact-analysis-for-business-continuity-Upstream-and-downstream-losses

Snedaker, S. (2011). Business Continuity/Disaster Recovery Plan Development. In *Business Continuity and Disaster Recovery Planning for IT Professionals*. Oxford, England: Butterworth-Heinemann.

Sobers, R. (2019, April 17). 60 Must-Know Cybersecurity Statistics for 2019. Retrieved June 1, 2019, from https://www.varonis.com/blog/cybersecurity-statistics/

Social Engineering Attacks: Common Techniques & How to Prevent an Attack. (2019, May 15). Retrieved from https://digitalguardian.com/blog/social- engineering-attacks-common-techniques-how-prevent-attack

Statista. (2014, February). Servers - annual failure rates | Survey. Retrieved from https://www.statista.com/statistics/430769/annual-failure-rates-of-servers/

StorageCraft Technology Corporation. (2019). Hardware Failure Survey Findings - StorageCraft. Retrieved from https://blog.storagecraft.com/hardware-failure/

Thune, K. (2019, May 17). IT Insurance: Cost, Coverage & Quotes for IT Business Insurance. Retrieved from https://fitsmallbusiness.com/it-insurance/

Toledo, J. (2018, May 29). Why Millions of Developers use JavaScript for Web Application Development? Retrieved from https://torquemag.io/2018/06/why-millions -of-developers-use-javascript-for-web-application-development/

United States Department of Labor. (1996, June 20). 1926.150 - Fire protection. Retrieved from https://www.osha.gov/laws-regs/regulations/standardnumber/1926/1926.150

Vijayan, J. (2018, May 29). What does a ransomware attack cost? Beware the hidden expenses. Retrieved from https://www.csoonline.com/article/3276584/ what-does-a-ransomware-attack-cost-beware-the-hidden-expenses.html

What is Cold Site? - Definition from Techopedia. (n.d.). Retrieved from https://www.techopedia.com/definition/998/cold-site

What is differential backup? - Definition from WhatIs.com. (n.d.). Retrieved July 7, 2019, from https://searchdatabackup.techtarget.com/definition/differential-backup

What's the Difference between Differential and Incremental Backups. (n.d.). Retrieved July 7, 2019, from https://www.easeus.com/backup-utility/ differential-backup-vs-incremental-backup.html

VMware. (n.d.). Back up a vCenter Server Appliance by Using the vCenter Server Appliance Management Interface. Retrieved from https://docs.vmware.com/en/VMware-vSphere/6.5/ com.vmware.vsphere.install.doc/GUID-8C9D5260-291C-44EB-A79C-BFFF506F2216.html

White, M. (2017, September 21). How to back up and recover vCenter Server Appliance (vCSA). Retrieved from https://www.veeam.com/wp-vmware- vcenter-server-appliance-backup-restore.html