The Final BCDR Plan

Our final project together!

Vanessa Bonner, Joseph Marquez, Zach Brown, Chris Armour, Zevin Alifi, Jordan Nutt

The University Of Advancing Technology

August 20, 2021

# 

# 

# Table of Contents

[**Table of Contents**](#_5rxarq1tyd22) **------------------------------------------------------------------------------------------- 2**

[**Company Info**](#_pxx5f58tu4sw) **---------------------------------------------------------------------------------------------- 7**

[Departments](#_lmf5unkkzi7g) ---------------------------------------------------------------------------------------------- 8

[Facility Description](#_54plx22guwv5) -------------------------------------------------------------------------------------- 9

[**Team Memo**](#_11e48qdpjbvw) **------------------------------------------------------------------------------------------------ 10**

[**Procedures**](#_51h3x3m1csou) **-------------------------------------------------------------------------------------------------- 11**

[Emergency Contact Information](#_qlo92q5kx4hm) ---------------------------------------------------------------------- 11

[Department Heads Contact](#_ecsdb7yu3kut) ----------------------------------------------------------------------- 11

[Damage Assessment Team](#_d0h39i3oocb3) ----------------------------------------------------------------------- 12

[Disaster Recovery Specialist](#_metiz6l0tbbs) --------------------------------------------------------------------- 13

[Technological Disaster Recovery](#_qx75xru54g2x) ----------------------------------------------------------- 13

[Environmental Disaster Recovery](#_1c3sdy7rfc4b) ---------------------------------------------------------- 13

[Emergency response](#_1ihrzj27lpps) ------------------------------------------------------------------------------ 13

[Crisis Management Team](#_e3rmvzn31qw2) ------------------------------------------------------------------------ 14

[Hazardous materials team](#_9bycgfd6if2v) ------------------------------------------------------------------------ 15

[Hospital](#_xp5bdx2b9dxz) --------------------------------------------------------------------------------------------- 15

[Ambulance](#_pnwvuq3ailvj) ----------------------------------------------------------------------------------------- 15

[Phone Line Down - Alternative Communications](#_yzzyd8r668ya) ------------------------------------------------ 17

[Alternate Worksite Activation](#_8gq7yg68lkip) ----------------------------------------------------------------------- 18

[Location](#_7q7gpgz7jtbj) -------------------------------------------------------------------------------------------- 19

[Personnel Requirements](#_b9kp4wxbciym) -------------------------------------------------------------------------- 19

[Personnel Contact Information](#_zcq2a6usm5tk) -------------------------------------------------------------- 19

[Site Backup Deployment](#_gl32yoh61i4t) ------------------------------------------------------------------------------21

[Cold Site Deployment Requirements](#_edjtqhc5utma) -----------------------------------------------------------21

[Warm Site Backup](#_b7c7uvlzxatb) ---------------------------------------------------------------------------------23

[Hot Site Backup](#_ig1q62lawrao) ------------------------------------------------------------------------------------24

[Mobile Backup](#_ry2xf5hk9sbr) -------------------------------------------------------------------------------------25

[Mirrored Site Backup](#_x13rptdrj6as) -----------------------------------------------------------------------------26

[Data Backup Procedure](#_1n7v5wudrjfn) --------------------------------------------------------------------------------30

[Backup Triggers](#_rr9pxud4erea) ------------------------------------------------------------------------------------30

[Backup Transfer Medium](#_vw9yhkg1rx96) -------------------------------------------------------------------------30

[Vital Datasets](#_flkg8bnvth9v) ---------------------------------------------------------------------------------------30

[Software](#_g08erkeqzz5d) ---------------------------------------------------------------------------------------------32

[Backup Policy](#_bfkbg7uq1obe) --------------------------------------------------------------------------------------33

[Incremental Backup](#_d18idu0xq6) ---------------------------------------------------------------------------33

[Full Site Backup](#_3nq96uhsmiv4) -------------------------------------------------------------------------------33

[Cloud Backup](#_48dqi2za946n) --------------------------------------------------------------------------------- 33

[Transfer Rates](#_d7owk6rj1yuu) ------------------------------------------------------------------------------------- 33

[**Action Plans**](#_jvglrswp1xx) **------------------------------------------------------------------------------------------------ 34**

[Overall Emergency Action Plan](#_wkkfadwf7mq) --------------------------------------------------------------------- 34

[External Elements](#_xxmsjfdpe1n5) ------------------------------------------------------------------------------------- 35

[Internal Elements](#_hi3fta1y0636) -------------------------------------------------------------------------------------- 36

[Disaster Declaration Statements](#_dbcl7g2h59sh) --------------------------------------------------------------------- 36

[Building Evacuation and Shelter](#_d4vi5ba1i90i) -------------------------------------------------------------------- 37

[Evacuation Maps](#_xy2afyysmvww) ---------------------------------------------------------------------------------- 37

[Procedure](#_53egwwarlyx6) ------------------------------------------------------------------------------------------- 37

[**Risk Assessment**](#_pz85i0r5p3k8) **------------------------------------------------------------------------------------------- 39**

[Business Functions](#_o51ulvp9zk17) ------------------------------------------------------------------------------------ 39

[Suppliers:](#_gwb2wh5vmszr) ------------------------------------------------------------------------------------------- 39

[Product Production:](#_5wg9xbq69va2) ------------------------------------------------------------------------------- 39

[Product Distribution:](#_65cv2wq8uldw) ----------------------------------------------------------------------------- 40

[Natural Threats](#_ynlzmxiz313v) ---------------------------------------------------------------------------------------- 40

[Vulnerability prioritization](#_grp84kogk3r7) ----------------------------------------------------------------------- 40

[Fires](#_nxu38xk0hte3) ------------------------------------------------------------------------------------------------- 40

[Power Outage](#_725jz1ki6orl) -------------------------------------------------------------------------------------- 41

[Haboob](#_de7k3jl62wc0) --------------------------------------------------------------------------------------------- 42

[Microburst](#_fnhut2ba006a) ------------------------------------------------------------------------------------------ 43

[Man-Made Threats](#_uza4fya1lc45) ------------------------------------------------------------------------------------- 43

[Vulnerability prioritization](#_dls8sofnowff) ----------------------------------------------------------------------- 43

[Equipment Failure](#_nsoenzwtqb3f) -------------------------------------------------------------------------------- 44

[The server room Fires](#_1lkiop7uk1v0) ---------------------------------------------------------------------------- 45

[Forgetting to Lock Things/Insider Threat](#_v71pbh8r0run) ------------------------------------------------------ 46

[Wildfires](#_sif9nwb5r35m) -------------------------------------------------------------------------------------------- 47

[IT and Technology-Based Threats](#_kznuwawusj16) ------------------------------------------------------------------- 47

[Vulnerability prioritization](#_hbey7jxpqbqy) ----------------------------------------------------------------------- 47

[Phishing](#_nfe860uhzmg3) -------------------------------------------------------------------------------------------- 48

[Ransomware](#_onmsu5qpofc7) --------------------------------------------------------------------------------------- 48

[Outages](#_9l9e79erdlb) --------------------------------------------------------------------------------------------- 49

[City Blackout](#_cie6kj59wvau) -------------------------------------------------------------------------------------- 50

[Hardware Failure](#_ulb0v5ok9zqb) ---------------------------------------------------------------------------------- 50

[Environmental Threats](#_ce6ovi9msto) -------------------------------------------------------------------------------- 51

[Biological](#_tu98wd95ewj8) ------------------------------------------------------------------------------------------ 51

[Infrastructure Threats](#_hqpwr99ha1x) --------------------------------------------------------------------------------- 52

[Building Infrastructure](#_inqpuws7yb9) --------------------------------------------------------------------------- 52

[Physical Security](#_jaahauhss84f) ----------------------------------------------------------------------------- 52

[RFID ID Badge Scanners:](#_mmkdbur07ujg) -------------------------------------------------------------- 52

[Security Staff:](#_go35tounbi1p) ---------------------------------------------------------------------------- 52

[Office Building Glass:](#_ku6x62ldtjo0) ------------------------------------------------------------------- 53

[Camera Blind Spots:](#_jw42qti8t45r) --------------------------------------------------------------------- 53

[Visitors:](#_1gluimncqoht) ------------------------------------------------------------------------------------ 53

[Utilities:](#_iszcqxpnxdkl) ---------------------------------------------------------------------------------------- 54

[Electrical](#_lytnky71e7zd) ---------------------------------------------------------------------------------- 54

[Sewerage](#_f8ut3ks217io) ---------------------------------------------------------------------------------- 54

[Water](#_lg5dum2gecjz) --------------------------------------------------------------------------------------- 55

[Office HVAC:](#_8wsoqzszyfcu) ----------------------------------------------------------------------------- 56

[Server Room HVAC:](#_48fhacxop94) -------------------------------------------------------------------- 56

[IT Infrastructure](#_tma0uiwksbrj) ----------------------------------------------------------------------------------- 56

[Open physical device ports (USB, Ethernet):](#_obkprwokp5xx) --------------------------------------------- 56

[Wiretaps](#_cwz0g9727qa4) ----------------------------------------------------------------------------------- 56

[Removable Storage Device](#_papkpmfvzlct) ----------------------------------------------------------------- 57

[Open Network Ports:](#_v6py2y2r2i1r) --------------------------------------------------------------------- 57

[Cloud Backups:](#_wvemayypxitu) --------------------------------------------------------------------------- 57

[**FEMA Risk Assessment**](#_xtlpikqtc68p) **--------------------------------------------------------------------------------- 58**

[Services](#_inqd6y6mtuoi) ------------------------------------------------------------------------------------------------- 58

[Hazards](#_e4qq5rsj9749) -------------------------------------------------------------------------------------------------- 58

[Human-Caused Hazards](#_vzy25bhbhvye) ------------------------------------------------------------------------------ 59

[Technological Hazards](#_ez9vvt6ntas4) -------------------------------------------------------------------------------- 59

[**Service Contracts**](#_5b2301n537ux) **----------------------------------------------------------------------------------------- 60**

[Dell](#_whkbh7byaxuz) ------------------------------------------------------------------------------------------------------ 60

[HP](#_enom4ikfwpyd) -------------------------------------------------------------------------------------------------------- 60

[Boldata](#_dxzivo98j1ic) -------------------------------------------------------------------------------------------------- 60

[We Sell Software Inc.](#_b4himi4wyvn1) ---------------------------------------------------------------------------------- 61

[Office Equipment](#_ojlgzuh4p6q2) -------------------------------------------------------------------------------------- 62

[Production Machines](#_n8gcyapejjhm) ---------------------------------------------------------------------------------- 62

[Bellah Law](#_jaxdakwa6kq8) --------------------------------------------------------------------------------------------- 62

[**Insurance and Legal**](#_ck41t554ji8r) **-------------------------------------------------------------------------------------- 63**

[Provider Information](#_dy9l85lnbqw) ----------------------------------------------------------------------------------- 63

[Coverage](#_pt98y77gh9bn) ------------------------------------------------------------------------------------------------ 63

[Insurance Gap Risk](#_mxlt9inj2pu0) ------------------------------------------------------------------------------------ 63

[Legal Counsel Information](#_imbgw4z5j98q) --------------------------------------------------------------------------- 64

[**Government Regulations**](#_o0dp42qw85l4) **-------------------------------------------------------------------------------- 65**

[Company Data Breach Regulations](#_dxc4b1u18cc) ------------------------------------------------------------------ 65

[Telemarketing Regulations](#_j2u5tzwom9gb) --------------------------------------------------------------------------- 65

[**Company Policies**](#_iz5d6tyfrp13) **----------------------------------------------------------------------------------------- 66**

[BC/DR Plan Updating](#_obkt3sqm4ljt) -------------------------------------------------------------------------------- 66

[BC/DR Plan Distribution](#_kq7kf12zlbw) ----------------------------------------------------------------------------- 67

[BC/DR Plan storage](#_9e9azg6n2l4a) ----------------------------------------------------------------------------------- 68

[Offsite Communications](#_iwe5i847orvr) ------------------------------------------------------------------------------ 68

[Disaster Notice](#_pipa43xtt5ls) ----------------------------------------------------------------------------------------- 70

[Data Breach Notice](#_93qw15qnraab) ------------------------------------------------------------------------------------ 70

[Data Backup](#_d5qm8x6mzv8o) -------------------------------------------------------------------------------------------- 70

[Incremental Backup](#_p54o907idt40) ------------------------------------------------------------------------------- 70

[Full Site Backup](#_x1zctp2134w0) ----------------------------------------------------------------------------------- 71

[Cloud Backup](#_ldokaiukwftq) -------------------------------------------------------------------------------------- 71

[Emergency Guidelines](#_zfc3q0fg21tj) -------------------------------------------------------------------------------- 71

[Building Evacuation](#_8qit5s2ed7y7) ----------------------------------------------------------------------------------- 72

[Personnel Accountability](#_lt6erf1pzkl4) ------------------------------------------------------------------------ 72

[Department Manager Procedure](#_811pomcvxgv0) ----------------------------------------------------------------- 73

[Shut-in Emergencies](#_6l0nxtmnl9om) ---------------------------------------------------------------------------------- 74

[Fire Systems Testing](#_8fkazpwvv1pt) ---------------------------------------------------------------------------------- 75

[Fire Sprinkler System Testing](#_qfn52z86helk) -------------------------------------------------------------------- 75

[Fire Alarm System Testing](#_46zfr2z8m9yx) ----------------------------------------------------------------------- 76

[Special Agent Extinguishing Systems](#_om24ilm6gpnz) ---------------------------------------------------------- 76

[Special Extinguishing Alarm Detection](#_mvuhye8ev3xc) -------------------------------------------------------- 77

[**Building Assessments**](#_ctswzyc7s2dl) **------------------------------------------------------------------------------------- 77**

[Assessment Forms](#_6mtmcohmiz41) ------------------------------------------------------------------------------------- 77

[Utility Monitoring](#_2b7hbkuu7uuy) ------------------------------------------------------------------------------------- 77

[Hazards](#_wxsoyz4joi1e) -------------------------------------------------------------------------------------------------- 79

[Hazardous Materials](#_z0lnyqmqpbju) ------------------------------------------------------------------------------ 80

[Physical Hazards](#_kbgwp53atyqb) ---------------------------------------------------------------------------------- 80

[Ergonomic Hazards](#_jtre1h7qbhqw) ------------------------------------------------------------------------------- 81

[Psychological Hazards](#_c68nrrl3vg66) --------------------------------------------------------------------------- 81

[Safety Hazards](#_5i1gj5j6kivo) ------------------------------------------------------------------------------------- 81

[Biological Hazards](#_txuckfqkdst5) -------------------------------------------------------------------------------- 82

[Hazardous Chemicals](#_uhix1447ytc3) ----------------------------------------------------------------------------- 82

[**Disaster Test Scenarios**](#_kiajl9sxuhog) **---------------------------------------------------------------------------------- 82**

[Nature-Based scenario](#_6rqbwp3z2hv2) -------------------------------------------------------------------------------- 82

[Man-Made Scenario](#_6ssrgf5h8b8x) ----------------------------------------------------------------------------------- 83

[Example Testing Memo](#_mgdq79gtwl3v) ------------------------------------------------------------------------------- 83

[**References**](#_ie0ju6idepex) **-------------------------------------------------------------------------------------------------- 86**

[**Appendix**](#_xxki7m8wx7j7) **--------------------------------------------------------------------------------------------------- 94**

[Employee Contact List](#_8z3qoi8yml8g) -------------------------------------------------------------------------------- 94

[Vendor Contact List](#_ccdvxu6tkbh9) ----------------------------------------------------------------------------------- 98

[Supplier Contact List](#_19nxarfpijdw) ---------------------------------------------------------------------------------- 98

[Blank DVD/CD/Case Suppliers](#_c3jh3nwc5rpt) ----------------------------------------------------------------- 98

[Box Suppliers](#_j5c4e1w22unl) -------------------------------------------------------------------------------------- 99

[Paper Supplier](#_ccro95nf12bs) ------------------------------------------------------------------------------------- 99

[Client Contact List](#_hhb2jag5w7v3) ------------------------------------------------------------------------------------ 99

[Product Distributors Contact List](#_jlyf1tazmfvh) ------------------------------------------------------------------ 100

[E.B Games - West Coast Stores](#_te5bw47pj45z) ---------------------------------------------------------------- 100

[Gamestop - East Coast Stores](#_dxdpqx8479ku) ------------------------------------------------------------------ 100

[Wal-Mart - Nationwide Stores](#_rqeykjdooonf) ----------------------------------------------------------------- 101

[Company Resources](#_9k1ow3z0ej2m) --------------------------------------------------------------------------------- 102

[Computer equipment](#_lxhwerwpupym) ---------------------------------------------------------------------------- 102

[Communication links](#_ehcsvudba3b1) --------------------------------------------------------------------------- 104

[Communications equipment](#_o3zwtp5a9ybz) ------------------------------------------------------------------- 104

[Office equipment](#_2qde4f8zy0xw) -------------------------------------------------------------------------------- 104

[Office supplies](#_lg0kkemfehrk) ----------------------------------------------------------------------------------- 105

[Production Equipment](#_oct15246zu8l) -------------------------------------------------------------------------- 105

[Facility Access - Key Cards](#_lz73b4t0iyca) ------------------------------------------------------------------------ 106

[Building 1 Access](#_97h95piya9r9) ------------------------------------------------------------------------------- 106

[Building 2 Access](#_i5v7n2ft00wl) ------------------------------------------------------------------------------- 106

[Building 3 Access](#_o141blvw2vxs) ------------------------------------------------------------------------------- 107

[Building Layouts](#_c2ynsbre3ag3) ------------------------------------------------------------------------------------- 108

[Figure 1 - Building 1 internal layout](#_skbspra7egc1) ---------------------------------------------------------- 108

[Figure 2 - Building 2 level 1 internal layout](#_97kzjsg57od1) ------------------------------------------------- 109

[Figure 3 - Building 2 level 2 internal layout](#_3qegmv9ajp99) ------------------------------------------------- 110

[Figure 4 - Building 3 internal layout](#_nlbjhbqigaii) ---------------------------------------------------------- 111

[Fire Suppression & Safety Equipment locations](#_gct219bzxlrm) ------------------------------------------------- 112

[Figure 5 - Building 1](#_6y9c5k221hll) ---------------------------------------------------------------------------- 112

[Figure 6 - Building 2 level 1](#_phbdvf4prnaa) ------------------------------------------------------------------- 113

[Figure 7 - Building 2 level 2](#_rkr07qwkl8sd) ------------------------------------------------------------------- 114

[Figure 8 -Building 3](#_dft9la9imote) ----------------------------------------------------------------------------- 115

[Building Evacuation Maps](#_kj6rtsjjd9ee) -------------------------------------------------------------------------- 116

[Figure 9 - Building 1](#_494q5tgj00o1) ---------------------------------------------------------------------------- 116

[Figure 10 - Building 2 Level 1](#_uybjiy2louuh) ----------------------------------------------------------------- 117

[Figure 11 - Building 2 Level 2](#_z0hs8g1g67pi) ----------------------------------------------------------------- 118

[Figure 12 - Building 3](#_sablercvy8cj) --------------------------------------------------------------------------- 119

[Network Diagrams](#_b9vy32pxxdo4) ----------------------------------------------------------------------------------- 120

[Figure 13 - Building 1](#_g000o1rp06jx) -------------------------------------------------------------------------- 120

[Figure 14 - Building 2](#_bqtxawcw233x) -------------------------------------------------------------------------- 121

[Figure 15 - Building 3](#_k04qazdehe7t) -------------------------------------------------------------------------- 122

[Financial Statements](#_dfdywglehgij) --------------------------------------------------------------------------------- 123

[Table 1 - Digiknights Financial Statement 2020](#_q30y893oubel) -------------------------------------------- 123

[Company Growth](#_hcnxdaq8nyqe) ------------------------------------------------------------------------------------ 124

[Figure 16 - Company Growth (5 Years)](#_r6nz2qlpxr6p) ------------------------------------------------------ 124

[Organizational Chart](#_n9bpznl582vt) --------------------------------------------------------------------------------- 125

[Assessment Forms](#_j5050s8wfmlr) ----------------------------------------------------------------------------------- 125

[Form 1 - Initial Asset Inventory and Assessment](#_wztxdp8fhf5m) ------------------------------------------- 126

[Form 2- Building Damage Assessment](#_26oq9v4yemta) ------------------------------------------------------ 127

[Form 3 -Individual Asset Assessment](#_3bgxaz5hsjl4) ------------------------------------------------------- 128

# 

# Company Info

DigiKnight Technologies Inc.

Telephone Number: 415-555-2668

Fax Number: 415-555-2622

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

**Background**

DigiKnight Technologies is a new company in the Silicon Valley region of California (indeed it is located within miles of Electronic Arts, Lucas Arts, and Cryptic Studios.) It was founded in 2000 by its current C.E.O. Carlton Smith, who realized the rapidly growing potential of game distribution. DigiKnight is not a publisher, nor does it create video games, rather it contracts with major publishers to rapidly produce the physical product (games) and coordinate their shipping to stores around the world. Though a new company, it has seen its sales grow extremely quickly over the last few years; as can be seen in the chart shown below.

## Departments

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

## Facility Description

**Building One** houses the administration department. It is a small single-story building of roughly 2000 square feet. At its entrance is a reception desk for guests visiting the facility, there is also a security guard post at the front door. There are a total of five offices, as well as bathrooms, and a medium-sized conference room.

**Building Two** houses the Sales, R&D, Shipping, and Advertising departments. It is two stories; with usable floor space roughly double that of the administrative building. Sales and Shipping are located on the bottom floor, along with another security guard post. On the top floor is the R&D Department and Purchasing Department. Instead of having individual offices for each employee, the departments are single rooms (2 per floor), with cubicles set up to give each employee some individual space. This helps to enhance team communication and cuts down on building costs.

**Building Three** is the production facility. It is 8000 square feet and consists of two rooms. In one room the maintenance team is facilitated to quickly provide any necessary maintenance to the machinery. The maintenance team also responds to maintenance issues in other buildings. In the main room of the building is the production equipment. It consists of NUMBER CD Stamping machines, each of which is capable of producing a large volume of discs. The discs then move into a diagnostic machine which randomly checks discs for quality control. Only discs and in-box materials are duplicated on-site. The company receives pre-made boxes from another manufacturer as well as silk-screened images to place on the CDs. Manuals and in-box ads are manufactured on-site using a high-speed printer. Once produced, a final machine places all items in a box and the box is sent down a conveyor belt to an employee station that places the finished boxes in a larger box for shipping to stores nationwide.

Also attached to Building 3 is the IT department, which contains the central servers for the facility.

# 

# Team Memo

Hello Team;

Maintaining the DR/BC plan is a team effort and for every quarter and drill exercise completed, we will be updating the plan with any new improvements approved through management. This will include items identified by employees and team leads during training. This could improve our response times, as well as recommendations from emergency response personnel and BC/DR contractors. Please make sure all documentation is updated and current for all department binders through team leads. Once a request is completed, a response from management will be requested for documentation review. This will ensure all departments are on the same page and eliminate any confusion in future operations. The reports will start at the lower levels, individual employees, and be reported up to team and department leads. From there the department leads will revise and forward recommendations to management for approval, and if approved, management will send the green light to update the plan to team leads. Once revisions are done by department heads, a revised document will be sent back to management for review and distribution to the main BC/ DR plan for all departments.

# Procedures

## Emergency Contact Information

### Department Heads Contact

In the event of an emergency please contact the 4 heads listed here. The Heads of the departments will make the continuing call if subordinate departments are needed.

* + Alicia McKellips - IT -415-555-8352
    - Carlton Smith - CEO & Founder - 415-555-7841
    - Brett Kelcey - Security - 415-555-3852
  + Linda Kraemer - Manufacturing -415-555-6161
    - Michael Winters - Maintenance Manager - 415-555-3970
    - Kenneth Gilliam - Shipping - 415-555-6431
    - Carlton Bowden -Research & Development - 415-555-3223
  + Diane Ford - Sales - 415-555-6312
    - Michael Churchill - Advertising - 415-555-3131
    - Katherine Cavenaugh - Purchasing - 415-555-3298
  + Mark Saunders - Administration - 415-555-8643
    - Bellah Law - Attorney - 602-252-9937

### Damage Assessment Team

* + Mark Saunders: Administration
    - Building 1: 415-555-8643 Ext 0180
  + Michael Winters: Maintenance
    - Building 3: 415-555-3970 Ext 0400
  + Linda Kraemer: Manufacturing
    - Building 3: 415-555-6161 Ext 0150
  + Alicia McKellips: IT
    - Building 3 IT Extension: 415-555-8352 Ext 0190
  + We Fix’Em Inc: Equipment Service Provider
    - 1-888-555-0567 Contract: WFDK4898
  + Insurancewide Company LLC: Nationwide Insurance Local Agent
    - (623) 873-1234
    - 5901 W Indian School Rd Suite 4 Phoenix, AZ 85033

### Disaster Recovery Specialist

#### Technological Disaster Recovery

Enterprise Technology Services

730 N 52nd St #100 Phoenix, AZ 85008   
602.426.8600

#### Environmental Disaster Recovery

HRS Restoration

170 S. William Dillard Drive, Building 6, Suite 118  
(602) 600-0407

### Emergency response

* + Phoenix Police Department
    - Emergency Phone Number: 911
    - Non-Emergency Phone Number: 602-262-6151
  + Arizona State Fire Marshal
    - Phone: 602-771-1400
  + Arizona Search & Rescue
    - Emergency: 911
    - SAR Coordinator 1-800-411-2336

### Crisis Management Team

The crisis management team is responsible for responding to all incidents, disasters, and crises. The team will be considered flexible so that they can adjust to the crisis at hand. The crisis management team listed below is the main point of contact for all crises at the company. If any other departments are required for more help within the crisis management team, it is the responsibility of the crisis management team-lead to contact department managers at their discretion. Departments of emergency response may also be informed depending on the situation.

* Mark Saunders: Administration
  + Building 1: 415-555-8643 Ext 0180
* Brett Kelcey: Security
  + Building 1: 415-555-3852 Ext 0170
* Michael Winters: Maintenance
  + Building 3: 415-555-3970 Ext 0400
* Linda Kraemer: Manufacturing
  + Building 3: 415-555-6161 Ext 0150
* Alicia McKellips: IT
  + Building 3 IT Extension: 415-555-8352 Ext 0190

### Hazardous materials team

* + Arizona Department of Environmental Quality Emergency Response Unit
    - Emergency: (602) 390-7894
    - Phone: (602) 771-4163

### Hospital

Banner - University Medical Center Phoenix

* Emergency Phone Number: 911
* Phone: (602) 839-2000
* 1111 E McDowell Rd Phoenix, AZ 85006

### Ambulance

AMR Central Arizona

* Emergency Phone Number: 911
* Phone: 1-844-30-3606
* 617 W. Main Street Mesa, Arizona 85201

## Phone Line Down - Alternative Communications

If landlines were to go down, we could utilize the VoIP option. As far as distribution lists, nothing would change other than adding 01 to the end of current numbers. We can set up a voice recording, informing the people calling in, that the menu options have changed and to please add 01 to the end of the number to reach their contact. That would trigger the VoIP phones to take the call and vice versa. If the Landlines and the ISP were to go out, we would go to a Cell Phone and Satellite connection. From here, we would have the heads of the departments with company-issued cells and numbers to be reached at. The internet connection would go through the satellite service provider to keep internet communications functioning. Cell phone alternatives can be implemented just as quickly. We would use a voice recording to inform contacts to add 02 to the end of their contact number. This would then redirect them to the cell number of the head of that department. This in turn would help simplify things. Email and Internet services could be conducted with these temporary wireless alternatives without many changes as repairs are being made to main systems.

**Alternatives to Landline Communication**

* Cell Phones - Cell Towers
* Handheld Two-Way Radios
* Building Intercom System
* Direct Person-to-Person Communication
* Physical Interdepartmental memos
* VoIP - Ethernet Phones - CAT5 Connection
* Satellite Connections - Starlink would provide an internet connection if all else fails. providing internet services to continue business as usual as well as voice communication.

## Alternate Worksite Activation

The Alternate worksite would be activated in the event of unforeseen outages due to; natural disasters, cyber-attacks, maintenance overhauls, fires, floods, etc. The phone tree with the heads of departments would be activated along with secondary personnel to become part of the skeleton crew to operate in the backup facility. The facility is updated Bi-weekly with data from the cloud servers to keep data up to date and minimize downtime. Once activated each department will execute their recovery plan simultaneously to quickly get the warm site up and running. The shipping department will reroute trucks to new locations for outbound product shipments. Sales will contact clients and inform them of production delays and give estimates of when deliveries and deadlines will be met. IT will update site systems and software to the current calendar date from cloud server backups as well as provide additional support to other departments and warranty service personnel. Manufacturing will get production lines and systems up and running and redirect raw supply trucks from the main site to the backup site, as well as take inventory of what’s on hand and what is needed. Maintenance will run through facility equipment and do the safety checks and procedures, as well as assist the production line with bringing systems online. Admin will contact employees and create a temporary emergency calendar schedule, as well as contact vendors for warranty support. Skeleton Teams will be established to keep services online at the backup site, and the recovery teams will work to bring the main site back online as soon as possible

**Personnel** **Requirements**

With the higher demand of running multiple sites, additional personnel will need to be hired. That would go for all departments and each site would have to have a team lead, Supplemental hires, temporary hires, and contract hires could be set up on an as-needed basis. Warm sites, Hot sites, and mobile sites would need to have dedicated personnel, even if at the minimum, it was just a skeleton crew. The equipment would need a central system that it backs up to, for all systems to be on the same clock and orders not to be lost or dubbed up creating confusion and loss of revenue.

### Location

* Secondary Warm Site Location With Skeleton Crew and Minimal Capabilities to continue production
* The Secondary site will be run by the heads and secondary backup per department and will submit the list of recommended team rosters per site.

### Personnel Requirements

* Heads of Departments w. Alternative backups.

#### Personnel Contact Information

* Admin
  + Mark Saunders: 415-555-8643 ext. 0180 Key Personnel
  + Rod Hatherly: ext 0181
* Sales
  + Diane Ford: 415-555-6312 ext. 0200 Key Personnel
  + Halle Branson ext. 0201
* Manufacturing
  + Linda Kraemer: 415-555-6161 ext. 0150 Key Personnel
  + Jessica Talen ext. 0151
* Research and Development
  + Carlton Bowden: 415-555-3223 ext. 0100 Key Personnel
  + Kurt Gossard ext. 0101
* Maintenance
  + Michael Winters 415-555-3970 ext. 0400 Key Personnel
  + Bell Rosenburg ext.0141
* Advertising
  + Michael Churchill 415-555-3131 ext. 0160 Key Personnel
  + Aaron McDowel ext. 0161
* Shipping
  + Kenneth Gilliam: 415-555-6431 ext. 0130 Key Personnel
  + Derrick Cunningham ext.0131
* Purchasing
  + Katherine Cavenaugh: 415-555-3298 ext. 0120 Key Personnel
  + Shay Robertson ext. 0121
* Security
  + Brett Kelcey: 415-555-3852 ext. 0170 Key Personnel
  + Frank Arrons ext. 0171
* IT
  + Alicia Mckellips: 415-555-8352 ext. 0190 Key Personnel
  + Luke McDowel ext. 0191
  + Allan Smith ext. 0192

## Site Backup Deployment

* Resources and deliveries have to be diverted to warm site
* Is a temporary site and can not keep up with all production deadlines
* Cost money to maintain takes away from the Net Gain
* Facilities can not house a full team

### Cold Site Deployment Requirements

* **Production line**
  + Printers - graphics, labels
  + Servers - Duplicate Software, Emails, Backups
  + Switches - Connect Machines to Network
  + Routers - Direct Traffic on Network
* **Shipping** 
  + Currier
  + Trucks
* **Raw Supplies** 
  + Boxes
    - Shipping Completed Products
  + CD’s
    - Copy Software
  + CD Cases
    - Put Completed CD’s In
    - Put Graphic Designs In
  + Paper
  + Ink
* **Phones**
  + Sales
  + Communications
* **Computers**
  + For Production Line
  + For Sales
  + For Admin
  + For Software Development

### Warm Site Backup

The warm site would have most of the same capabilities as the main site and can be run with a skeleton crew for short periods to keep production moving forward. The site is backed up bi-weekly from the cloud with the data from the main site to keep an up-to-date duplicate of current clients, orders, and deadlines that need to be met. The warm site is a little more than half the size of the main site, so full production can not be sustained at 100%, but can continue to operate. The main purpose of the site is to eliminate downtime and mitigate the loss of data, clients, and revenue due to unforeseen circumstances and provide a recovery site to keep DigiKnight Technologies Co. operational.

Pros.

* Provides a temporary work site while repairs are made to the main site
* Production keeps moving forward
* Minimizes downtime of services
* Has Current data on hand - eliminating data loss
* Provides a second redundant location for emergencies
* Can be run with a skeleton crew

Cons.

* Does not have a full-size production line, causing Production to slow down by over 50% due to limited resources and personnel
* Shipping has to be rerouted to warm site to continue production shipments

**Equipment**

* Computers
* Printers
* Servers/Routers (All types)
* Phones
* Cloud Services

### Hot Site Backup

To begin with, a Hot Site is also called a “Dynamic Backup or an Active Backup.” A hot site is another replicable system of the main site, where the hot site is a backup site that holds everything that the main site has. The pros of a hot site are that it usually has all the equipment in the hot site location and has connectivity to the main site’s database, is fully redundant, and will have no data loss. A hot site is usually used for business-critical applications, the hot site also has a logical application of the entire environment. The cons about hot sites are that they are used for emergencies if the main site experiences a disaster and they have to move employees and employers to a specific building. The hot site is a replicated version of the main building’s systems in the event of a disaster so a business can resume work while working to fix the main servers' issues.

* Computers
* WorkPhones
* USB
* Switches/Routers
* HVAC system for the servers
* Office space (if applicable)
* Cloud network, software, AWS

### Mobile Backup

Amazon AWS Snowball Mobile Backup Solutions

AWS Snowball is an offline data transfer and edge computing solution allowing for quick data transfer to AWS servers. This backup solution comes as a physical device with 80 terabytes of usable storage and 40 vCPUs. With this device, the company could quickly transfer all of the data from the 10 Dell PowerEdge r620 servers and set up a backup server solution. This device can be rack-mounted alongside the existing servers after taking delivery from Amazon. Transferring the data to AWS servers is quick and simple by either mailing the device to Amazon or physically delivering the device to an Amazon AWS site. AWS Snowball may also be used to restore data from AWS servers to the company’s local servers.

Cost Breakdown:

* + Upfront cost:
    - 1 year $15,330
    - 3 year $38,325
  + Device Usage Cost:
    - $500 per Usage
    - $50 per day on demand
  + Additional Fees
    - $125 per day after 10 days
    - $0.03 per GB transfer cost from AWS to local servers

### Mirrored Site Backup

* Computer equipment
  + Administrative Computers
    - 10 x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad-Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10
  + Sales Computers
    - 15 x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad-Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10
  + Research and Development Computers
    - 3x Custom Computer Builds
      * Intel Core i7-4470
      * 32 GB of RAM
      * 4 TB SSD Hard Drive
      * NVIDIA GForce GTX 1660 Video Card
      * Gigabit Network Card
      * Dual 26 Inch Monitors
      * Windows 10 Professional
  + Shipping Computers
    - 4x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad-Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10
  + Advertising Department Computers
    - 5x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad-Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10
  + IT Department Computers and Servers
    - 5x Workstations
      * Intel Quad-Core i7-4470
      * 16 GB of RAM
      * 1 TB SSD Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 21 Inch Monitor
      * Windows 10
    - 10x Servers
      * PowerEdge R620
      * 16 GB of RAM
      * 3 X 2 TB Hard Drive (configured to RAID 5)
      * Windows Server 2016
      * Dual Gigabit Network Cards
      * 15 Inch Monitor
  + Manufacturing
    - 10 x Custom Built Machinery Computer Systems
* Network Equipment
  + 10 x Cisco Network Switches
  + Cisco Network Router
* Production Equipment
  + Number CD Stamping Machine
  + CD diagnostic Machine
  + High-Speed CD Manuals Printer
  + Shipping Conveyor Belt

## Data Backup Procedure

### Backup Triggers

* Physical - Bi-weekly -calendar-based.
* New Contract - Full Backup Before preceding as a best practice situation.
* Contract Completion - Systems check and backup recovery archive.
* Wednesday/ Sunday - Full Local Backup Split between days
* Saturday - Incremental Cloud backup
* Quarterly - Full Cloud Backup
* Emergency Situations - Deploy external HDD backups and systems checks

### Backup Transfer Medium

Company data will be backed up through two types of backups, local and cloud. Local backups will utilize the Company’s internal Category 5 cable backbone to complete data transfer. When backing up data to the cloud, the Company will make use of the dual OC3 fiber lines connected at the ISP’s Demarc point.

### Vital Datasets

* Main Server
* Local Sales Database
* Account information
* Employee information
* Business Contact Information
* Employee and Business Contracts
* Shipping and Deliveries Information
* Company Insurance and Warranty
* Company Financial Records
* Product Software Installation Media and Product Keys
* Computer Backups (Optical Media)
* Employee Personal Email Accounts
* Employee Business Email Accounts
* Email Correspondence with Customers
* Email Correspondence with suppliers
* Company Website Design
* QuickBooks Computer Records
* Customer Database
* Supplier Database
* Corporate Database
* Customer Payment Information (including Credit Cards)

### Software

Windows 2016 built-in backup for the servers. AWS or Azure for the backup of files using these types of technologies to help conduct the backup.

### Backup Policy

#### Incremental Backup

To accommodate for data loss the company will use incremental backups throughout the business day to allow for vital company information to be replicated immediately.

#### Full Site Backup

Every Wednesday and Sunday the main company site will complete a full site backup to external removable Hard drives. This full backup will occur after hours and the full data package will be split into two parts.

#### Cloud Backup

A full warm site backup to the cloud will be transferred once every quarter. In between these cycles the company will utilize incremental backups to update data that has been changed between cycles. This incremental backup will occur once per week on Saturday after hours.

### Transfer Rates

At 100 megabytes per second as the transfer rate. At that speed it will transfer:

1 GB in 10 seconds

10 GB’s in 100 seconds

100 GB’s in 1,000 seconds

1 TB in 10,000 seconds

2 TB’s in 20,000 seconds

20,000 seconds = 333.33 minutes

333.33 minutes = 5.56 hours (approx 5 and a half hours)

Here are the times for transfer rates from 90 megabytes per second to 140 megabytes per second:

90 Mb/s —- 6.17 hours

100 Mb/s — 5.56 hours

110 Mb/s — 5.05 hours

120 Mb/s — 4.63 hours

130 Mb/s — 4.27 hours

140 Mb/s — 3.97 hours

# Action Plans

## Overall Emergency Action Plan

* + - What will be the major actions needed to be taken to execute successfully
      * Contact the two main heads for the BC/DR plan
        + IT Head - Manager: Alicia McKellips 415-555-8352
        + Research and Development Head - Manager: Carlton Bowden 415-555-3223
      * Inform all major parties of the current situation.
      * Redirect all major parties to new facilities
      * Get the backup facility up and running to continue meeting orders
      * Repair the main facility as quickly as possible to get back up to 100%
    - How both internal and external crises will be handled
      * Internal crises will be handled by upper-echelon staff and individual tasks will be delegated down by department heads.
      * External crises will be analyzed and managed by Sales teams and Research and Development to keep us agile and be able to pivot to secondary suppliers, shipments, and vendors if the situation arises.
        + Keeping an up-to-date research plan on market costs and delivery prices.

Supplies needed to carry out production

Software needed to produce orders

Shipping costs and alternative solutions

## External Elements

Shipping

Inform them of the current situation and if need to redirect them to backup facilities to continue with outbound deliveries.

Supplies

Inform them of the current situation and if need to redirect them to backup facilities to continue with inbound deliveries.

Clients

Inform them of the current situation, and what this will mean for their orders.

3rd Party Contractors

Do we need to hire more people?

## Internal Elements

* Data
  + Client Data Accounts and Orders
* Personnel
  + Payroll
  + Shift Schedule
* New Location Relocation
  + Do we need anything from our main facility that we do not have in our backup facility?
* Hardware
  + What systems are needed to continue business operations?
* Software, Production, Shipping

## Disaster Declaration Statements

Customers, Investors, Shareholders, Vendors, Community

Due to unforeseen circumstances, Digiknights is having technical difficulties and is advising that some services and client shipments might be delayed. Digiknights will send out periodic updates as the situation is remedied and will be available; For contact on any questions, clients might have. Please use the information provided to reach out to us during this temporary delay in operations.

Employees, Contractors

During this time of difficulty, we must strive to provide great customer service and answer any questions to our clients, investors, and suppliers to give them peace of mind. Our foremost priority is to our customers and getting Digiknights up and running at 100% in the shortest time possible. Please keep your teams ready and alert to updates and events that may arise from this difficult situation and pass on all information that will aid in recovery. Utilize your department heads to relay updates periodically to upper echelons to provide detailed information on what current developments have arisen, what solutions are being implemented, and what the ETA is on correcting the problems to get us to 100% and back on track.

## Building Evacuation and Shelter

### Evacuation Maps

Available in Appendix Figure 9, 10, 11, 12

### Procedure

In the event of a building evacuation, it is the responsibility of each department manager to direct their team to safety by following the designated evacuation procedure. If the department manager of a team is not present during the evacuation then the responsibility will fall to another Evacuation leader present in the corresponding building. All employees and visitors must evacuate the building to predetermined safe points that are designated in the evacuation procedure plans. Evacuation notifications will be distributed through the following three forms of communications: Fire Alarm, PA Intercom System, and phone calls. Departments of emergency response may also be informed depending on the situation.

* Mark Saunders: Administration
  + Building 1: 415-555-8643 Ext 0180
* Brett Kelcey: Security
  + Building 1: 415-555-3852 Ext 0170
* Diane Ford: Sales
  + Building 2 Level 1: 415-555-6312 Ext 0200
* Kenneth Gilliam: Shipping
  + Building 2 Level 1: 415-555-6431 Ext 0130
* Michael Churchill: Advertising
  + Building 2 Level 2: 415-555-3131 Ext 0160
* Katherine Cavenaugh: Purchasing
  + Building 2 Level 2: 415-555-3298 Ext 0120
* Carlton Bowden: R&D
  + Building 2 Level 2: 415-555-3223 Ext 0100
* Michael Winters: Maintenance
  + Building 3: 415-555-3970 Ext 0400
* Linda Kraemer: Manufacturing
  + Building 3: 415-555-6161 Ext 0150
* Alicia McKellips: IT
  + Building 3 IT Extension: 415-555-8352 Ext 0190

# Risk Assessment

## Business Functions

### Suppliers:

2 weeks of Downtime limit

A delay in supplies for product development would lead to a decrease in company productivity. If suppliers were unable to supply the company for an extended period of time the company would suffer a loss. While the company does keep a stock on hand as a buffer in case there is a delay, the production team would eventually run out of these supplies. This would cause a total shutdown of product production and distribution.

### Product Production:

7 days of Downtime limit

The products produced by the company are vital to the company and its clientele. If production were to cease function so would product distribution. This would cause downtime not only for the company but our clients that require our products to continue operations.

### Product Distribution:

2 weeks of downtime limit

The distribution of products produced by the company to retailers around the country is important to the company but not vital. If the distribution channels were to be slowed or temporarily stopped the company would be able to recover. A stockpile of products would get created at the company which would need immediate delivery after distribution channels were reopened.

## Natural Threats

### Vulnerability prioritization

1. Fires
2. Microburst
3. Power Outages
4. Haboob

### Fires

Arizona’s hot and dry climate makes it hard to notice wildfires, and with these environmental conditions in place, It makes fires much more likely to become a conser. Fires destroy everything and can be devastating to a company's product, infrastructure, and personnel health.

**Probability of Occurrence**

Somewhat Likely, Tho fires are common in Arizona, They burn year-round in the state, but are most numerous and typically burn the largest swaths of land during spring and summer. You don’t hear about too many companies being heavily affected, but they are very common.

**Company Loss Analysis**

**Impact:** Complete Loss of infrastructure, Loss of Data, Operations Halted, Product Destroyed, Clients Lost

**Upstream:** Can Lock up the grid with emergency response units. Damage Personnel Properties, Cause Panic, Evacuation protocols.

**Downstream:** Can destroy infrastructure, inventory, records, data, causing loss of clients

### Power Outage

While rare here in phoenix they can be pretty bad if something were to go wrong. Unless we have a UPS system and have multiple backups or protective surge plugs there isn’t much to worry about.

**Probability of Occurrence**

Very Likely, Phoenix has experienced rolling blackouts in its history, with no power you can not run your business, power your grid, keep communication open.

**Loss Analysis**

**Impact:** Halt to Operations, Loss of revenue, loss of clients, damage to reputation.

**Upstream:** Grid Lock, Prevention of employees to reach work, Loss of communication, disconnection from the grid, loss of information.

**Downstream:** Loss of customers, loss of revenue, loss of data, potential loss of vendors, damaged reputation.

### Haboob

Haboob storms don’t happen year-round but can occur randomly, associated with microburst and more frequent in the summer and monsoon times. The likelihood of this being a seasonal constraint threat is unlikely, so countermeasures should be taken so we are prepared for such a disaster. The potential damage they can cause is not just limited to data loss but also loss of life. In 2011 Arizona Department of Public Safety Officers responded to a 16 car pile-up on Interstate caused by A blinding dust storm, causing three pileups involving dozens of vehicles where at least 15 people were injured, and one man was killed. This locked the roadways on the interstate i-10 between Tucson and Phoenix.

**Probability of Occurrence**

Very likely to occur in Arizona, They are a desert native storm that can cause a lot of damage due to its high wind speeds, loss of visibility, and panic it creates within people.

**Loss Analysis**

**Impact:** Slowdown of operations, Shut down of business for the day, loss of revenue, property damage

**Upstream:** Products not to reach destinations due to loss of visibility and gridlock, employees not being able to reach work.

**Downstream:** Can halt operations causing loss of revenue, loss of clients, potential loss of vendors, and shut down the business.

### Microburst

Historically Arizona has had very destructive Microburst ranging from, flash flooding, tornados, record high temps, record cold temp, extremely high winds, large hail storms, severe lightning storms, resulting in property damage, business shutdowns, gridlocks, power outages, severe injuries, and loss of life.

**Probability of Occurrence**

Somewhat Likely because they occur each year between June 15 and Sept. 30, Damage to infrastructure, Products, Data, Revenue, Customers, Business Operations, Vendor Relationships.

**Loss Analysis**

**Impact:** Loss of revenue, loss of infrastructure, shut down of businesses, loss of employees

## Man-Made Threats

### Vulnerability prioritization

1. Equipment Failure
2. Server room Fires
3. Forgetting to Lock things/Insider threat
4. Wildfires

### Equipment Failure

If equipment is not properly maintained or cared for this could be the biggest cause of all the company's network issues.

**Probability of Occurrence**

Equipment Failure can affect an entire company depending on what equipment fails. Equipment has a high maintenance cost to make sure that it doesn’t die out on the company. Causing profit loss and or data loss to the company

**Loss Analysis**

**Impact:** This failure can range depending on the severity of the situation. If a wire to a computer came unplugged it’s not a big issue but if a bigger piece of equipment could go down it could potentially cost hundreds of dollars per minute of downtime.

**Upstream:** Potential profit loss depending on how important that equipment is. If you lose cables it could be a huge profit loss as it could potentially take down your entire network.  
**Downstream:** Customers won’t have access to your website/products if the internal network is down so the customers will not come back to the company if they see us down.

### Server room Fires

Servers run Hot! especially here in Arizona. Server room fires could potentially lose the company a lot of money in maintenance, downtime, and recovery costs due to the extreme heat Arizona has. It’s best to maintain adequate air conditioning and monitor Hot and Cold aisles in the server room.

**Probability of Occurrence**

Server room fires can be started from many things such as Electrical Failure, Subfloor wiring, Overheated electronics, And other various fires that may occur but if we are talking electronic fires. 78% of non-home electronic room fires originated from electronic equipment according to the National Fire Protection Association.

**Loss Analysis**

**Impact:** The biggest damage to a company's network is if a server room were to go up in flames. All server data could be lost and operational costs could be high for recovering and replacing the broken equipment.

**Upstream:** Potential downtime and data loss of the company and its supplies  
**Downstream:** The customers won’t have easy access to the company if they are a seller of products.

### Forgetting to Lock Things/Insider Threat

Insider threat whether unintentional or intentional is a serious threat that could compromise an entire company.

**Probability of Occurrence**

Forgetting to lock things or Insider threat is the risk of physically leaving an important door unlocked for those who probably should not have access to that room. By forgetting to lock a door, You are putting the company's data at risk of potential tampering.

**Loss Analysis**

**Impact:** If IT staff forgets to lock a door and someone were to wander into the server room the potential damage could be high as all your highly valuable data could be contained in the room where this threat could access. No matter if there was malicious or non-malicious intent the risk is not worth taking.

**Upstream:** Your stakeholders will lose money as well as you can lose money if an incident were to occur and take down your network.   
**Downstream**: Your customers wouldn't be at too much risk depending on the severity of a risk.

### Wildfires

Here in Arizona almost half of 500 communities are at risk of a wildfire as some buildings are built next to flammable landscapes.

**Probability of Occurrence**

In about 500 communities studied by the Arizona Department of Forestry and Fire Management, 42% of homes were at high risk for wildfires and 44% were at moderate risk.

**Loss Analysis**

**Impact:** Wildfires will cause the most infrastructure damage from the building to the operations as a wildfire cannot be controlled as easily as a server room fire. Wildfires will cost a loss in the recovery of data as you will likely have to rebuild systems in a new building to continue operations and return backups.

**Upstream**: Fire departments will lose resources trying to protect people's homes from further damage caused by Wildfires  
**Downstream**: People could potentially lose their homes and belongings to a fire.

## IT and Technology-Based Threats

### Vulnerability prioritization

1. Phishing
2. Ransomware
3. Outages
4. Blackout
5. Hardware Failure

### Phishing

**Probability of Occurrence**

Very likely, these attacks are very common and any company can fall for them as nearly ⅓ do fall for them.

**Loss Analysis**

**Impact:**  Loss of revenue, Data loss, Potential Business affiliations, and potentially loss of employees

The most common hacking technique, From an article by safeguard cyber, In the 2019 Verizon data breach investigation. It states that ⅓ of all cybersecurity breaches involve phishing. Making is very common to fall for. Putting the suppliers and customers at risk equally as if a company falls for such an attack they could lose a lot of data and money from suppliers and customers.

### Ransomware

**Probability of Occurrence**

Very likely, Any company is vulnerable to these attacks as they are just as common if not more common than phishing attempts when it comes to security.

**Loss Analysis**

**Impact:** Loss of revenue, Data loss, Potential business affiliations.

**Upstream:** For the suppliers, if a company were to fall. They could lose stock or private documents having to do business with the company. Potentially losing trust with that company and losing money  
-**Downstream**: A customer's data could be leaked out by the attacker if they were to get such data.

### Outages

**Probability of Occurrence**

Very likely The Internet is constantly going down be it from new construction, power outages, software updates, or tech refreshes and systems crashes. This is very common in the IT field and issues like this are dealt with daily.

**Loss Analysis**

**Impact:** Loss of Net Revenue, Google makes 108k every minute that it’s online, every minute can be multiplied by that number to calculate total Net Revenue lost.

With the internet down we could potentially lose clients, revenue, and vendors or products.

### City Blackout

Blackouts rarely happen in the state of Arizona and they aren’t too much of a problem in AZ alone as companies like APS and SRP work together to make sure customers never experience long-term power outages.

**Probability of Occurrence**

Rarely happens in Arizona, a backup generator would help for the blackout.

### Hardware Failure

**Probability of Occurrence**

The least detrimental out of all of the most of the time but every company will experience hardware failure eventually. Tech gets old and needs replacing.

**Loss Analysis**

**Impact:** Minor data loss if it’s a hard drive. Money loss for replacement parts if needed.

While probably the most common with a blog post who polled over 400 of their partners with 99% of them saying they experienced a hardware failure. It’s not the most detrimental since in the same blog post most of the failures are caused by hard drives. Which are easily recoverable for a company.

## Environmental Threats

### Biological

Biological threats from viruses such as COVID-19, flu, and the common cold can lead to major health concerns. Depending on the spread of the virus throughout the company we could see a varying degree of loss of productivity. From one person being sick to the entire company being shut down while the buildings are sanitized. The company must also be aware of the effects of viruses concerning our suppliers. During the COVID-19 Pandemic, businesses saw a shortage of supplies affecting 39.2% of essential businesses.

**Probability of Occurrence**

Covid-19 (Pandemic): More of a global situation but a situation that affected all of the world.

**Loss Analysis**

**Impact:** Covid-19 (Pandemic): Practically killed every business in America alone that didn’t have any form of backup plan.

**Upstream:** Any type of environmental disaster that occurs by a third-party supplier can cause a huge mishap. We will lose a lot of potential profit made by our partnership if our upstream is affected by an environmental disaster.  
**Downstream:** With a disaster, We will lose out on a lot of profits made during that time whether we are affected directly by it or not. If we offer services to our community or key customers we will not have their business as they deal with the disaster.

## Infrastructure Threats

### Building Infrastructure

#### Physical Security

##### RFID ID Badge Scanners:

Without the use of ID verification through facial recognition or the Security Room ID badges can be used for infiltration onto the Company’s premises. Through the use of card skimmers ID badge data can be copied and duplicate cards made. Simple human error can lead to cards being stolen and used by criminals.

##### Security Staff:

Insider threat is a very real possibility and can come from employees, former employees, Security staff, Contractors, etc. With security staff, It’s best to look for credible staff with a pretty good reputation and work experience in security to prevent further threats from other sources. They are to protect the employing parties’ assets from spying or forward-facing threats.

##### Office Building Glass:

Glass comes in a variety of different types and strength ratings. From tempered glass to impact-resistant and bulletproof glass. The use of the wrong type of glass outside and within the company’s buildings can have a detrimental effect. The use of tempered glass in the lobby while cost-effective does leave the building vulnerable to attacks. With a simple rock, an intruder could break the glass opening up the facility. On the other hand, having bulletproof glass for all windows would create an extraneous expense for the company and possible liabilities in the event of an emergency.

##### Camera Blind Spots:

Surveillance cameras come in a variety of flavors each with its own strengths and weaknesses. Within the facility, you would ideally want to be able to access an IP Camera with pan and zoom capabilities, to monitor a large room, like the production line, outside the buildings, and common areas that are accessible to the public. While these cameras allow you to maneuver and observe a wide area, their field of view is limited to the direction they are pointed to at any given moment. This creates blind spots that could be exploited to gain access to restricted and sensitive areas. The second downfall of these cameras is that they are vulnerable to outside threats, can be easily disabled with gum or spray paint, and can be accessed to spy on the company and or be taken offline if not properly secured. Third, not only are CCTV security camera systems very expensive, they only observe what's happening and need a human entity to do the reporting if something is outside of normal operations. This is why most of the time you see large out-of-date fixed position cameras placed in hallways and outside buildings pointed at the most common and high traffic areas with the hopes of deterring a breach given its obvious vulnerabilities. To mitigate the possibilities of that happening the cameras should be placed redundantly with the objective being if one fails then the other can still give us eyes on the targeted area. This can be accomplished with multiple views of hallways, rooms, and perimeters of the facilities. Paired with other security measures, like automated door locks, alarm systems, access badges, and segregation of access to facilities, blind spots and breaches can be mitigated to a more acceptable risk factor. This will keep the budget down, and eliminate the need to purchase state-of-the-art surveillance equipment for a small business operation.

##### Visitors:

Allowing visitors past the lobby of the company leaves the company open for corporate espionage. Visitors could conceal their intentions through various social engineering techniques to gain access to sensitive sections of the building. This would allow them to access company data and record the building’s layout.

#### Utilities:

##### Electrical

Electricity is a vital requirement for the company to continue operating. Without electricity, the building of the entire company would cease its daily functions. This type of threat can come from various sources including the city power grid, backup generator, and faulty wiring.

##### Sewerage

There is to consider, of course, mechanical wear that damages the integrity of the property’s sewer systems, such as leaks, corrosion, or cracks in the pipes. They must be maintained by dedicated plumbers, whether they are on staff or. The maintainers will also account for the surrounding area that might have obstacles that prevent flow. Without proper

##### Water

Under Federal Law, employers must provide potable water that employees can consume. Potable water includes tap water that is safe to drink, and employers are not allowed to make employees pay for water that is provided. However there are some areas in the states where the tap water does not meet the drinking water requirements, thus a drinking fountain or bottled water must be provided. This is because the OSH Act created the Occupational Safety and Health Administration (OHSA), which sets and enforces protective workplace safety and health standards. So if the water goes out production stops. A disruption in the water supply is a serious health and safety issue. Employers are required to clean washroom facilities, toilets must flush, and employees must be able to wash their hands. If the water goes out employers must provide an alternative to comply with OSHA standards. This can be done with portable hand washing stations, portable toilets, and portable trailers that have been converted to provide temporary facilities while the water issues are repaired.

##### Office HVAC:

Office HVAC is a necessity in the summer months of Arizona. The Phoenix Metropolitan area has seen temperatures of over 120 degrees Fahrenheit. The loss of HVAC would result in lower employee productivity and increased aggression. If the temperatures within the building were to rise to a dangerous level all employees would need to be sent home until the HVAC system was repaired.

##### Server Room HVAC:

The airflow provided by the Server Room HVAC system is vital for continuous operation. This system removes contaminants through stages of air filtration including HEPA. The Arizona desert is full of dust particles which would comprise the electronics in the server room without this filtration. The HVAC system also removes the hot air from the server racks keeping them cool. If the system were to completely fail the company may suffer data loss from overheating servers and the possibility of a fire.

### IT Infrastructure

#### Open physical device ports (USB, Ethernet):

##### Wiretaps

Through the use of network monitoring devices and keyloggers, the company’s data can be transmitted offsite through network tunnels created by these devices. Common network monitors take the form of an inline ethernet device. However, network monitoring devices and keyloggers have become harder to spot. Companies are making devices that are disguised inside the end of USB cables or embedded in other computer peripherals such as keyboards.

##### Removable Storage Device

These devices allow for one of the easiest forms of corporate espionage. These incredibly small devices allow for the company’s data to be copied and exfiltrated off the property. Storage devices can also be used as malware delivery devices that could infect the entire company network. Custom storage devices are also available on the open market. One of these devices is the USB Rubber Ducky which can design itself to a computer as a different peripheral allowing it to execute a custom coded payload.

##### Open Network Ports:

Open Network Ports are vulnerable to hacker port scanning, where they use software like Nmap, to find which ports are open in a given computer system, and whether or not an actual service is listening on that port and then an attempt to exploit potential vulnerabilities in any services they find. Once in, the attacker can inject their malicious malware to gain control over said systems, remove sensitive data, plant rootkits, or just fly under the radar and capture packets over a long period of time. This can be mitigated by closing non-essential ports, monitoring port traffic, and filtering. This doesn't mean an attack won’t happen but active security monitoring can streamline the reaction time it would take to respond to such a threat.

##### Cloud Backups:

Data must be protected in multiple ways. Making sure confidential data isn’t exposed to the outside world is just as crucial as the assurance that it remains intact. If hardware or human failure occurs, a cloud backup can guarantee some resolve. If there is any data loss, the company can simply roll back to their existing backup. Depending on the frequency at which you create the backups, and how many redundant ones are made, less work has to be done to get back where you left off.

# FEMA Risk Assessment

## Services

## 

## Hazards

* Geological - Earthquake, Tsunami, Landslide
* Biological - Pandemic Disease, Foodborne Illnesses

## Human-Caused Hazards

* Accidents - Workplace Accidents, Entrapment/Rescue (Machinery, Water, Confined Space, High Angle), Transportation Accidents.
* Intentional Acts - Demolition, Civil Disturbance (Riot), Verbal or written threats of violence (Bomb Threats/Shootings), Lost/Separated Person, Child Abduction, Kidnapping/Extortion,

## Technological Hazards

* Information Technology - Loss of Connectivity, Hardware Failure, Lost/Corrupted Data, Application Failure
* Utility Outage - Communications, Electrical Power, Water, Gas, Steam, Heating/Ventilation/Air Conditioning
* Fire/Explosion - Fire (Structure, Wildland), Explosion (Chemical, Gas, or Process failure)
* Hazardous Materials -Hazardous Material spill/release, Radiological Accident, Hazmat Incident off-site, Transportation Accidents
* Chain Interruption - Supplier Failure, Transportation Interruption

# Service Contracts

The company has several service contracts for its various pieces of equipment. This is a listing of those contracts, along with other important information.

## 

## Dell

The contract with Dell covers all computer systems purchased from them. The contract includes same-day service if a request call comes in before 3 PM; otherwise, the contract guarantees next-day service.

The contract number is: 42368131588-DGK and expires every year on December 29th. It can be renewed every year without changing the contract terms. Each computer purchased is numbered with the serial number DGK12389-#, where the # symbol represents the number of the computer (there are currently 25 Dell systems in the office, labeled 1 – 25). If service is needed, the user should call 1-888-555-5897.

## HP

Similar to the Dell contract, this contract covers all HP and Compaq computer systems. It was negotiated during a period of time where special deals were given to customers, so it includes 24-hour service, three-hundred-sixty-five days a year, with no additional charge.

The contract number is: DGK-13548253 and expires every year on February 22nd. It can be renewed every year without changing the contract terms. Each computer purchased is numbered with the serial number DGK55879-#, where the # symbol represents the number of the computer (there are currently 22 HP and Compaq systems in the office, labeled 1 – 22) If service is needed, the user should call 1-888-555-5237.

## Boldata

Boldata systems is a smaller company, and as such only offers a service contract that covers sending maintenance personnel on-site Monday through Friday between the hours of noon and five. It is not an ideal service contract, but it is enough to cover the few systems owned by the company.

The Contract number is DGK1161 and expires every three years on March 9th. Systems have the serial number DGK - # where the # symbol represents the number of the computer (there are currently 3 Boldata systems in the office, labeled 1 – 3) If service is needed, the user should call 1-888-555-1497.

## We Sell Software Inc.

All of the software owned by DigiKnight is offered 24-hour customer support telephone service through this company. It covers all office, sales, administration, and other software programs. Every piece of software has its serial number embedded into the program, so further writing it down is not necessary. The contract is numbered DK823892. If software service is needed the individual may contact 1-888-9876.

## Office Equipment

These machines are covered by Office Equip Inc. The service contract covers normal working hours at the company and will even send a new unit if it is necessary (requiring of course that the user then mail back the broken unit).

The contract number for all office equipment is OEIDKG-125. The contract is currently set to expire on November 7th, 2007. By the decision of Office Equip Inc. all devices owned by the company are given the serial number DGK191. The number to call for service is 1-888-555-1576.

## Production Machines

All of the production machines are serviced on-site by the maintenance staff. If the maintenance staff is unable to affect a repair then it contacts We Fix’Em Inc, who can be reached at 1-888-555-0567. The machines have no serial numbers because they were custom-built, but the contract number in case it is ever needed is WFDK4898.

## Bellah Law

If legal counsel is needed the company keeps Bellah Law Office on retainer to handle LLCs, Corporations, Contracts, Leases, Employment Agreements.

5622 W Glendale Ave, Glendale, AZ 85301

8:00 AM - 5:00 PM M-F Office Hours

Contact info/ Phone: 602-252-9937, Website: <https://bellahlaw.com/>

# Insurance and Legal

## Provider Information

AmTrust Contact Information:   
 1 (877) 528-7878 - Customer service  
212.499.0100 - General information  
216.643.5969 - Corporate fax

## Coverage

Cyber Liability -$1,500 /year   
Workers Compensation - $400-$800 /year  
Business owner’s policy - $1,191 /year

In a security-related event, A breach can cost thousands of dollars in damages, and With AmTrust Cyber insurance They will cover a wide range of cyberattacks such as those listed above and assist in addressing the attacks during and after the event to restore data integrity.

## Insurance Gap Risk

An insurance gap could spell trouble when it comes to computer security, as hardware and recovery require a lot of money. A potential insurance gap could be a breach of Personally identifiable information. While an insurance company would protect data in the event of a data breach, outside of that if you were to have some personal information leak, that is very unlikely to be covered under insurance

## Legal Counsel Information

If legal counsel is needed the company keeps Bellah Law Office to handle LLCs, Corporations, Contracts, Leases, Employment Agreements. If our legal team can not meet what is required then private legal contractors will be augmented as needed.

Bellah Law

5622 W Glendale Ave, Glendale, AZ 85301

8:00 AM - 5:00 PM M-F Office Hours

Contact info/ Phone: 602-252-9937, Website: <https://bellahlaw.com/>

# Government Regulations

## Company Data Breach Regulations

Under Arizona Data-Breach Notification Laws A.R.S. §§ 18-551 and 18-552 DigiKnight Technologies is required to notify the individuals involved in the breach. If the breach affects more than 1,000 individuals then Digiknight must notify the three largest nationwide consumer reporting agencies. If more than 100,000 individuals are affected or the cost of providing notice exceeds $45,000 DigiKnight must inform the attorney general through a written letter and release a public notice on the company website.

## Telemarketing Regulations

The company is restricted in the hours that it may contact consumers under the Telephone Consumer Protection Act of 1991 (TCPA) 47 CFR 64.1200(c)(1). Any residential telephone subscriber may not be contacted before the hours of 8 a.m. or after 9 p.m. in their timezone. This means that any current or potential clients may not be contacted by phone when outside of these hours. Digiknight must keep timezone considerations in mind when contacting individuals.

# Company Policies

## BC/DR Plan Updating

After every Emergency Response Drill and situation, the After actions survey and response should be reviewed, and the plan should be updated with any insights and steps taken to improve the current plan. The recommendations of response teams and employees should be taken into account and a strategy to implement them into our current plan should be developed. Team Leads should discuss what happened during responses and what they observed in their sections and how they would react differently if something was found lacking. Things to take into account would be:

1. How long it took for employees to react to the emergency alarms.
2. How long it took to pass out emergency supplies.
3. How long it took to secure workstations.
4. How long it took to evacuate the building.
5. How long it took to reach the secure assembly area.
6. How long it took to take accountability of all personnel.
7. How long it took to secure crucial systems.
8. How long it took to take accountability of all crucial systems.
9. How long it took to report all departments to Management.

The reasoning behind this approach is to build experience and quicken response times, make notes on where the plan needs more attention to detail, and train employees on their part in an emergency. If details are overlooked in the initial planning then the after actions report will show us where we need to improve our plan. A prepared team response is more efficient than one caught off guard. By taking notes on how long every step of the plan took. We also can track how well we are responding to emergencies and track our improvement linearly over time as we run drills.

With these steps, we can actively keep our plan up to date with all the information gathered and continuously improve upon our plan. Any new findings can be implemented as needed and any changes that need to be executed can be added.

**Additional Information**

An After Actions Survey can be created specifically for different response situations.

Team Meetings can be held to discuss ways to improve upon the current Emergency Response Plan, What worked well, and what could use some revamping.

Outside Contractors can be brought in to run different safety drills with the company.

Training dummies can be purchased to run different evacuation scenarios for a deeper level of preparation and more life-like training situation.

## BC/DR Plan Distribution

Hello, team.

Plan updates can be distributed through digital documents like pdfs, verbal conferences with your team, or physical papers. Clearly define what departments and people will be affected the most by the plan updates. Create pre-emptive answers to concerns you expect your team to have.

## BC/DR Plan storage

Documents containing information about the BC/DR plan and other various emergency documents must be backed up via digital copy. Digital copies are the most important asset for our documents as they allow for quick changes, previous version backups, and quick and easy access if an employee or someone else needs it.

Physical Documents are less important than digital but still important especially if it’s an escape plan that we need to put up in the hallways of the building.

## Offsite Communications

The company needs to maintain good crisis management through a work from home policy given current events. Team members must follow a ruleset when engaging with each other, but especially so off-site. There are many means for this such as communicating only through secure means like encrypted communication platforms. Routine stress testing of security systems so that potential vulnerabilities are discovered ahead of time puts us at an advantage over those who actively would try to compromise our business. Secure online and offline backups of important company records are crucial as well.

## Disaster Notice

In the event of a disaster and depending on the size of the disaster, We will need to inform employees, customers, stakeholders, and possibly the media. It is important to make sure that all legal requirements are met when assessing the damages of a disaster so we can minimize the cost of recovery so we can put more focus on it. The first people to know about a breach would be the employees as it affects how they will work, next would likely be stakeholders or those who hold stock or share into the company as they put money into investing into the company. Next would be the general public which includes media and customers to alert them of the potential risk they are at from the aforementioned disaster.

## Data Breach Notice

Under Arizona Data-Breach Notification Laws A.R.S. §§ 18-551 and 18-552 DigiKnight Technologies is required to notify the individuals involved in the breach. If the breach affects more than 1,000 individuals then Digiknight must notify the three largest nationwide consumer reporting agencies. If more than 100,000 individuals are affected or the cost of providing notice exceeds $45,000 DigiKnight must inform the attorney general through a written letter and release a public notice on the company website.

## Data Backup

### Incremental Backup

To accommodate for data loss the company will use incremental backups throughout the business day to allow for vital company information to be replicated immediately.

### Full Site Backup

Every Wednesday and Sunday the main company site will complete a full site backup to external removable Hard drives. This full backup will occur after hours and the full data package will be split into two parts.

### Cloud Backup

A full warm site backup to the cloud will be transferred once every quarter. In between these cycles the company will utilize incremental backups to update data that has been changed between cycles. This incremental backup will occur once per week on Saturday after hours.

## Emergency Guidelines

In the event of an emergency, Employees will be expected to follow the safety guidelines we set out for them but before that, they need to know some policies and procedures before taking the steps to safety.

Employees are expected to follow the guidelines that were taught to them in training.

* + Secure your Stations
    - Shutdown Machines
    - Grab your ID Cards
    - Close and lock Drawers
  + Use the exit procedures for your section and department
    - Follow the emergency exit guilds posted at the doors and exits
    - Avoid obstructions and hazardous conditions that may cause injury
  + Assist fellow employees to exit safely from your sections
* Never take shortcuts on procedures.
  + Taking shortcuts can lead to sloppy work in ensuring proper safety for everyone in the building
* Make sure that all emergency exits are clear for everyone to evacuate in an emergency.
  + Do not place boxes or other obstructions that could block exits or walkways.

## Building Evacuation

In the event of an emergency, the building doors will default to open, allowing people to safely exit the building. Sensitive areas will be automatically locked by default with safety releases if inside, one to safely exit to the evac area.

### Evacuation Maps

Available in Appendix Figure 9, 10, 11, 12

### Personnel Accountability

When an emergency alarm sounds, calmly move towards the exits identified for your section or area on the emergency evacuation maps posted at every door and exit and proceed to the emergency gathering area. Once you have arrived at the emergency gathering area, your team lead will take accountability for their department and report that up to management. In the event the team lead is not there, the first person at the evacuation gathering point will take accountability for their department, report up to management, and identify the team lead was not at the gathering point. Once everyone is accounted for, shuttles will pick up employees and bus them to a pre-designated safety point (nearby hotel) for final accountability call, and information gathering while safety crews run through the structures.

### Department Manager Procedure

In the event of a building evacuation, it is the responsibility of each department manager to direct their team to safety by following the designated evacuation procedure. If the department manager of a team is not present during the evacuation then the responsibility will fall to another Evacuation leader present in the corresponding building. All employees and visitors must evacuate the building to predetermined safe points that are designated in the evacuation procedure plans. Evacuation notifications will be distributed through the following three forms of communications: Fire Alarm, PA Intercom System, and phone calls. Departments of emergency response may also be informed depending on the situation.

* Mark Saunders: Administration
  + Building 1: 415-555-8643 Ext 0180
* Brett Kelcey: Security
  + Building 1: 415-555-3852 Ext 0170
* Diane Ford: Sales
  + Building 2 Level 1: 415-555-6312 Ext 0200
* Kenneth Gilliam: Shipping
  + Building 2 Level 1: 415-555-6431 Ext 0130
* Michael Churchill: Advertising
  + Building 2 Level 2: 415-555-3131 Ext 0160
* Katherine Cavenaugh: Purchasing
  + Building 2 Level 2: 415-555-3298 Ext 0120
* Carlton Bowden: R&D
  + Building 2 Level 2: 415-555-3223 Ext 0100
* Michael Winters: Maintenance
  + Building 3: 415-555-3970 Ext 0400
* Linda Kraemer: Manufacturing
  + Building 3: 415-555-6161 Ext 0150
* Alicia McKellips: IT
  + Building 3 IT Extension: 415-555-8352 Ext 0190

## Shut-in Emergencies

In the event of a shut-in emergency because of severe weather or natural disaster, emergency supplies will be distributed to employees. This will include Flash Lights, MRE’s, Water bottles, emergency blankets, and cots for extended stays. All buildings will have their stash of emergency supplies in the red lockers by exits and emergency supply closet, and each building will have a designated gathering point. Each building will also have walkie-talkies and emergency generators for small devices and communication between buildings, loved ones, and emergency channels. Team Leads will be trained with emergency procedures in the event of an emergency. This will include how to batten down the hatches for the building, making sure all equipment is properly secured, and all personnel is accounted for.

## Fire Systems Testing

Note: Fire Sprinkler maps available in Appendix Figure 4, 5, 6, 7, 8

\*\*IMPORTANT\*\*

Before any testing can be performed by a licensed inspector, Fire Protection must be called to put the building on Test mode. Fire Protection will require a code provided by the property management company. Failure to put the building into Test mode before conducting testing will result in the Fire Department being deployed which may result in a fine.

### Fire Sprinkler System Testing

* Visual Inspection
  + Performed by Staff Quarterly
  + Scope:
    - Visual inspection of system pressure, check gauges, rusting components, evidence of a leak, damage, etc.
* Complete NFPA 25 Inspection
  + Performed by Licensed Contractor Annually
  + Scope:
    - Water Flow, Valve activation, etc.
* 5-year Inspection
  + Performed by Licensed Contractor every 5 years
  + Scope:
    - Internal valve and pipes, check all valve covers and branch lines for corrosion, etc.

### Fire Alarm System Testing

* Visual / Verify No Troubles Inspection
  + Performed by Staff weekly
  + Scope:
    - Check the lights on the panel, supervisory signals weekly, etc.
* Annual Inspection
  + Performed by Licenced Contractor
  + Scope:
    - Test all connected devices: smoke detectors, heat detectors, batteries, circuits, etc.

### Special Agent Extinguishing Systems

* Semi-Annual Inspection
  + Performed by Licenced Contractor
  + Scope:
    - FM200 system
* Annual Inspection
  + Performed by Licenced Contractor
  + Scope:
    - FM200 system

### Special Extinguishing Alarm Detection

* Visual Inspection
  + Performed by Staff Monthly
  + Scope:
    - FM200 System
* Annual Inspection
  + Performed by Licenced Contractor
  + Scope:
    - FM200 System

# Building Assessments

## Assessment Forms

Complete Assessment forms found in Appendix

Form 1 - Initial Asset Inventory and Assessment

Form 2- Building Damage Assessment

Form 3 -Individual Asset Assessment

## Utility Monitoring

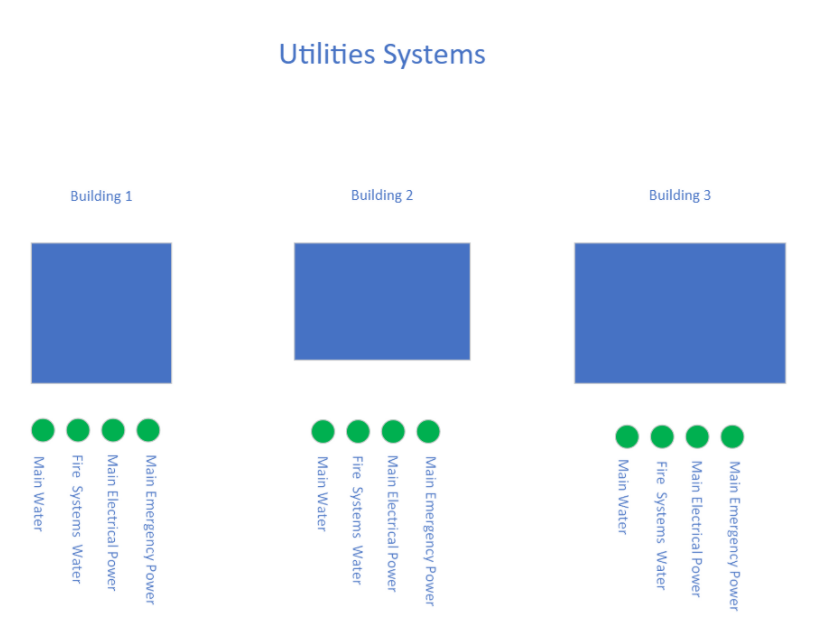
The Guard Post will have a utility monitoring grid that will be continuously monitored and in the event of a failure, an alarm will sound as well as a color-coded light identifying what systems and where they are located, and why they failed.

Green Solid = All Systems Operating Normally

Yellow Blinking = System Down for Scheduled Maintenance

Red Blinking = System Reporting Error

Red Solid = System Down/ Failure



* Building 1
  + Main water
  + Fire systems water
  + Main Power
  + Emergency Power
* Building 2
  + Main water
  + Fire systems water
  + Main Power
  + Emergency Power
* Building 3
  + Main water
  + Fire systems water
  + Main Power
  + Emergency Power
* Guard Post
  + Main water
  + Fire systems water
  + Main Power
  + Emergency Power

## Hazards

Hazardous Materials - Examples of these products include materials that are flammable, explosive, oxidizing, poisonous, infectious, corrosive, or dangerously reactive

### Hazardous Materials

* Batteries (Lithium)(Heavy)
* Fuel Canisters
* Cleaning Supplies
* Compressed Air
* Medical Waste ( Bathrooms Biohazard Bins )
* Trash Bins

### Physical Hazards

* Radiation- Ionizing, EMF’s, Microwaves, Radio Waves
* High Exposure to Sunlight and Ultraviolet rays
* Exposure to hot and cold temperature extremes
* Constant Exposure to Loud Noise
* Impaired Visibility due to poor lighting or obstruction
* Objects in walkways
* Unsafe or Misused Machinery
* Excessive Noise
* Falls ( Loading Docks )
* Water/ Liquid Spills causing slippery floors
* Fires

### Ergonomic Hazards

* Repetitive Movement over and over
* Improper Setup of workstation and chairs - ( poor posture )
* Poor Design of equipment
* Workstation design
* Manual handling of large or heavy objects ( frequent lifting, having to use too much force, awkward movements)

### Psychological Hazards

* Shift Work
* Work Loads
* Dealing with the public
* Harassment
* Discrimination
* Threat of Danger and Violence

### Safety Hazards

* Slip and Trip ( spills, extension cords, working from heights)
* Inappropriate Machine Guarding
* Equipment Malfunctions
* Electrocution ( Electrical discharge from improperly grounded or damaged machines, power surges, wall outlets)

### Biological Hazards

* Bacteria/ Viruses ( Sick Employees )
* Blood and other body fluids ( Employees )
* Insects ( Bites )
* Plants ( Pollen, Poison )
* Animals ( Local Wild Life ) (Droppings)
* Grey/ Black Water Flooding from Bathrooms (Sewage)
* Server Room Overheating (Cold Isle fail)
* Electrical Fire From Shortages and frayed cords
* Battery Swelling, exploding, and containment failures

### Hazardous Chemicals

* Lithium ( Batteries )
* Alcohol ( Hand Sanitizer )
* Ammonia ( Cleaning Supplies )
* Difluoroethane, trifluoroethane, Tetrafluoroethane, or butane ( Canned Air )
* Diesel Fuel ( Generator )(Trucks)

# Disaster Test Scenarios

## Nature-Based scenario

In the event of a flash flood which can occur in Arizona during monsoon season. Your safety is a priority in this situation rather than the building. As a flash flood starts coming people need to remain calm as panic can make things worse in almost any situation. But if a flash flood is developing quickly you have to drop what you are doing and find safety on a higher floor to prevent the water from climbing up to you as fast. Get anyone out of low areas and up into higher parts of the building for safety and from there just wait. Don’t move from where you are unless it’s to go higher into the building.

## Man-Made Scenario

In the event of a bomb threat, one of the most important things to keep in mind is to remain calm. Causing a panic will lead situations to escalate much further and possibly make things worse. In this scenario, information and communication are critical. Whoever found the threat or got the call, needs to immediately notify authorities and higher staff about the situation so the higher-ups can spread the information out to authorities and other staff so everyone can stay calm. When talking to proper authorities, Tell them all the information from, voice, age, sex, any background noise, any suspicious bagging. Exact words are needed if the threat is made via a call. If a suspicious item is found on the location, do NOT touch the item. Leave it and keep a safe distance away from it as your goal is to safely find a way out of the building or find a safe spot in general. As part of training for this situation, we will have staff watch bomb threat training videos so they can understand the risks and procedures for dealing with this threat as safety is the number one priority.

## Example Testing Memo

Good Evening Sir,

Today's Emergency Response Drill (ERD) will take place between 8 am - 12 am. The drill should only take around 15 minutes from start to finish with 30 minutes afterward for review and reflection. The Alarm will sound in the allotted time and a Stopwatch timer for each department and building will begin. The scenario for the Emergency Response Situation will be randomly selected and vary from rolling blackouts to earthquake and extreme weather, and be executed as soon as the alarm sounds. Each department will have to follow their emergency response procedures, safely exit the building and gather in the assembly area for accountability. Once accountability is completed the department head will report to management, and their timer will stop. Once all departments from each building report to manage the building’s timer will stop. Once all buildings are evacuated, and all Departments have reported in, the drill will be completed and the reflection and review period will begin. This will cover all the response times with all departments to see who is falling behind and who is leading in emergency response. The review will also request that the employees complete a small survey on their individual experience, what they found easy and what they found difficult, and if they have any comments on where we could improve on. Keeping employee morale in mind, the department with the best response time will receive a free lunch and get a plack with their department's response time and bragging rights for their wall. This is not meant to be a competition but just a little encouragement and incentive to help the company be well-practiced and prepared for when the situation arrives.

# 

## 

# References

1. 18-551 - Definitions. (2018). In Arizona legislature. https://www.azleg.gov/ars/18/00551.htm
2. 18-552 - Notification of security system breaches; requirements; enforcement; civil penalty; preemption; exceptions. (2018). In Arizona legislature. https://www.azleg.gov/ars/18/00552.htm
3. 2020 ransomware statistics, data, & trends. (2020, July 18). PurpleSec. https://purplesec.us/resources/cyber-security-statistics/ransomware/
4. A Guide to Critical Infrastructure Security and Resilience. (2019, November). CISA. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
5. ALDAY, J. (2017, February 9). Disaster recovery: Cold sites, hot sites, and why do I care? Cima Solutions Group. https://www.cimasg.com/2017/02/disaster-recovery-cold-sites-hot-sites-and-why-do-i-care/
6. Amazon. (n.d.). Amazon FSx for Windows file server. Amazon Web Services, Inc. https://aws.amazon.com/fsx/windows/
7. AmTrust Financial. (2021). Cyber insurance, cyber liability | AmTrust financial. AmTrust Financial. https://amtrustfinancial.com/insurance-products/cyber-liability
8. Anne Marie Helmenstine, Ph.D. (2018, January 8). Canned air isn't actually air. ThoughtCo. https://www.thoughtco.com/whats-in-canned-air-3975941
9. Arizona communities at high risk during wildfire season. (2020, July 24). Cronkite News - Arizona PBS. https://cronkitenews.azpbs.org/2020/07/24/arizona-communities-high-risk-wildfire-season/
10. Arizona has lost $1B from data breaches since 2005 • Arizona mirror. (2020, August 5). Arizona Mirror. https://www.azmirror.com/blog/arizona-has-lost-1b-from-data-breaches-since-2005/
11. AWS. (2021). AWS snow family | Physical devices to migrate data into and out of AWS | Amazon web services. Amazon Web Services, Inc. https://aws.amazon.com/snow/
12. Barry, J. (2021, February 19). Texas power outage disaster raises concerns about whether it could happen in Arizona. AZFamily. https://www.azfamily.com/news/texas-power-outage-disaster-raises-concerns-about-whether-it-could-happen-in-arizona/article\_d13184c4-730d-11eb-849e-2f79d1935e2d.html
13. Business Impact Analysis. (2007, May 25). Request Rejected. https://cdn.ttgtmedia.com/searchSecurityChannel/downloads/443\_Disaster\_04\_(2).pdf
14. City Of Phoenix. (2018). Fire Protection Systems and Equipment Inspection, and Maintenance. Official Website of the City of Phoenix, Arizona. https://www.phoenix.gov/firesite/Documents/Fire%20Protection%20System%20Inspection%20Frequency%20Guide.pdf
15. Coco-Stotts, K. (2020, January 30). The top 5 threats to your IT infrastructure. JumpCloud. https://jumpcloud.com/blog/five-threats-infrastructure#cookie-accept
16. CONTINUITY OF OPERATIONS PLAN (COOP). (2010, April). Gadsden County Sheriff's Department. https://gadsdensheriff.org/pdf/emergency\_mgt\_docs/Continuity%20of%20Operations%20Plan.pdf
17. Dcurwin. (2019, April 24). What is Azure backup? - Azure backup. Developer tools, technical documentation, and coding examples | Microsoft Docs. https://docs.microsoft.com/en-us/azure/backup/backup-overview
18. Department of Corrections (DOC). (2019). Strategic Plan. Washington State Department of Corrections (DOC). https://www.doc.wa.gov/docs/publications/100-SP001.pdf
19. Department of Emergency and Military Affairs. (2019). Emergency management. https://dema.az.gov/emergency-management
20. EKBERG, N. (2016, October 17). A business continuity and disaster recovery checklist. NYSTEC. https://www.nystec.com/insights/a-business-continuity-and-disaster-recovery-checklist/
21. Embroker. (2020, August 26). How much does cyber insurance cost?. https://www.embroker.com/blog/cyber-insurance-cost/
22. Equipment out of order. (n.d.). smart-eam.com. https://smart-eam.com/en/polomka/
23. FEMA. (2020, July 30). Risk assessment. Plan Ahead for Disasters | Ready.gov. https://www.ready.gov/risk-assessment
24. Gerd Simon, (2018, May) Understanding and Mitigating Risks to Data Center Operation https://www.dotmagazine.online/economic-engine-digital-infrastructure/mitigating-risks-to-data-center-operation
25. Hardware failure | Arvig blog. (2020, March 3). Arvig Business. https://www.arvigbusiness.com/for-business/hardware-failure-why-it-happens-and-how-it-impacts-business/
26. Hardware failure survey findings - StorageCraft. (2013, September 27). StorageCraft Technology, LLC. https://blog.storagecraft.com/hardware-failure/
27. HARRIS & COMPANY. (2019, September 18). Workplace hazardous materials information system (WHMIS). go2HR. https://www.go2hr.ca/health-safety/safety-basics/workplace-hazardous-materials-information-system-whmis
28. Historical Arizona storms of the 20th century. (n.d.). National Weather Service. https://www.weather.gov/psr/Arizona\_historic\_storms
29. Holton, L. J. (2018, July 5). The disadvantages of CCTV. It Still Works. https://itstillworks.com/12083564/the-disadvantages-of-cctv
30. Information Security. (2021). Threat likelihood and vulnerability assessment - Information security. Google Sites. https://sites.google.com/site/infosecsecurity201/information-security-risk-management/risk-assessment-activities/threat-likelihood
31. Insider Threat Mitigation for U.S.Critical Infrastructure Entities: Guidelines from an Intelligence Perspect. (2021, March). Home. https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf
32. Maricopa. (2021). Most common natural hazards. Maricopa County, AZ | Official Website. https://www.maricopa.gov/5143/Most-Common-Natural-Hazards
33. NWS Phoenix storm event summaries. (n.d.). https://www.weather.gov/psr/eventsummaries
34. Omnisecu. (2021). Types of backup sites - Hot site, warm site, cold site. Types of Backup Sites - Hot Site, Warm Site, Cold Site. https://www.omnisecu.com/ccna-security/types-of-backup-sites.php
35. OSHA. (1980, September 12). 1910.165 - Employee alarm systems. | Occupational safety and health administration. Occupational Safety and Health Administration. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.165
36. Osha. (2021). Workers’ Rights. Occupational Safety and Health Administration. https://www.osha.gov/sites/default/files/publications/osha3021.pdf
37. Peterson, S., & Kirvan, P. (2018, September 18). Developing an emergency communications plan: A template for business continuity planners. SearchDisasterRecovery. https://searchdisasterrecovery.techtarget.com/Developing-an-emergency-communications-plan-A-template-for-business-continuity-planners
38. RiskSense (n.d.). RiskSense: Full Spectrum Risk-Based Vulnerability Management. https://risksense.com/wp-content/uploads/2018/12/Protecting-Arizona-Against-Cyber-Threats.pdf
39. S., S. (2018, June 15). Are employers required to provide drinking water to employees? Petrillo & Goldberg Law. https://www.petrilloandgoldberg.com/frequently-asked-questions/are-employers-required-to-provide-drinking-water-to-employees/
40. Segue Technologies. (2016, October 11). The three stages of disaster recovery sites. https://www.seguetech.com/three-stages-disaster-recovery-sites/
41. Snedaker, S., & Rima, C. (2013). Business continuity and disaster recovery planning for IT professionals (2nd ed.). Syngress Press.
42. Status. (2020, August 7). How to communicate during an organizational change [7 best practices]. Status Articles. https://status.net/articles/change-management-communication/
43. Stone, A. (2020, September 28). Phishing attacks are what percentage of cyber attacks? Secure Communication Channels & Social Media | SafeGuard Cyber. https://www.safeguardcyber.com/blog/phishing-attacks-are-what-percentage-of-cyber-attacks
44. The most common causes of server room fires might surprise you. (2017, June 8). Cooling Power. https://coolingpowercorp.com/news/common-causes-server-room-fires-might-surprise/
45. Tim Hoffer, (2018, Feb 16). The Main Causes of Underground Infrastructure Damage https://www.softdig.com/blog/main-causes-underground-infrastructure-damage/
46. Trimmer, R.(n.d.). YouTube. https://www.youtube.com/watch?v=bI-dO7RI3lE
47. Tweney, D. (2013, August 16). 5-minute outage costs Google $545,000 in revenue. VentureBeat. https://venturebeat.com/2013/08/16/3-minute-outage-costs-google-545000-in-revenue/
48. U.S. Bureau of Labor Statistics. (2021, March 3). Comparing the experiences of essential and nonessential businesses during COVID-19: The economics daily: U.S. Bureau of Labor Statistics. https://www.bls.gov/opub/ted/2021/comparing-the-experiences-of-essential-and-nonessential-businesses-during-covid-19.htm
49. V-amallick. (2021, May 4). Support matrix for the MARS agent - Azure backup. Developer tools, technical documentation, and coding examples | Microsoft Docs. https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix-mars-agent
50. Waterlogic. (2017, November 15). Drinking water - The US law | Waterlogic. Water Coolers and Dispensers for Office and Waterlogic. https://www.waterlogic.com/en-us/resources-blog/drinking-water-the-law/
51. Wpadmin. (2020, June 10). Differences between a cold, warm and hot disaster recovery site. OTAVA. https://www.otava.com/blog/what-is-the-difference-between-a-cold-warm-and-hot-disaster-recovery-site/

# Appendix

## Employee Contact List

**CEO & Founder:**

Carlton Smith 415-555-7841

**Administration**

Manager: Mark Saunders

Main Phone line: 415-555-8643

| Employees: | Phone Extension |
| --- | --- |
| Mark Saunders | 0180 |
| Rod Hatherly | 0181 |
| Bea Holdeman | 0182 |
| Susan Marcotte | 0183 |
| Kendra Bell | 0184 |
| Dillon Sommer | 0185 |

**Sales**

Manager: Diane Ford

Main Phone line: 415-555-6312

| Employees: | Phone Extension |
| --- | --- |
| Diane Ford | 0200 |
| Halle Branson | 0201 |
| Natasha Lowe | 0202 |
| Thomas Baird | 0203 |
| Lorna Hastings | 0204 |
| Dwayne Roby | 0205 |
| Pam Millard | 0206 |
| Katie Barnes | 0207 |
| Leonard Filby | 0208 |
| Helen Reese | 0209 |

**Manufacturing**

Manager: Linda Kraemer

Main Phone line: 415-555-6161

| Employees: | Phone Extension |
| --- | --- |
| Linda Kraemer | 0150 |
| Jessica Talen | 0151 |
| Andrew Saunders | 0152 |
| Cassie Johnson | 0153 |
| Annette Watson | 0154 |
| Marty Kitzman | 0155 |

**Research & Development**

Manager: Carlton Bowden

Main Phone line: 415-555-3223

| Employees: | Phone Extension |
| --- | --- |
| Carlton Bowden | 0100 |
| Kurt Gossard | 0101 |
| Sam Jarosz | 0102 |
| Corey Bogdan | 0103 |
| Anne Mcloskey | 0104 |

**Maintenance**

Manager: Michael Winters

Main Phone line: 415-555-3970

| Employees: | Phone Extension |
| --- | --- |
| Michael Winters | 0400 |
| Bell Rosenburg | 0141 |
| Adam Loudy | 0142 |
| Katelin Griffin | 0143 |
| Lance Addams | 0144 |
| Jeffery DeVane | 0145 |

**Advertising**

Manager: Michael Churchill

Main Phone line: 415-555-3131

| Employees: | Phone Extension |
| --- | --- |
| Michael Churchill | 0160 |
| Aaron McDowel | 0161 |
| Owen Mill | 0162 |
| Allison Bell | 0163 |
| Rebecca McClintock | 0164 |
| Jessica Williams | 0165 |

**Shipping**

Manager: Kenneth Gilliam

Main Phone line: 415-555-6431

| Employees: | Phone Extension |
| --- | --- |
| Kenneth Gilliam | 0130 |
| Derrick Cunningham | 0131 |
| Evan McAllister | 0132 |
| Kevin Albright | 0133 |
| Brent Kastner | 0134 |

**Purchasing**

Manager: Katherine Cavenaugh

Main Phone line: 415-555-3298

| Employees: | Phone Extension |
| --- | --- |
| Katherine Cavenaugh | 0120 |
| Shay Robertson | 0121 |
| Robert White | 0122 |
| Ian Wolf | 0123 |

**Security**

Manager: Brett Kelcey

Main Phone line: 415-555-3852

| Employees: | Phone Extension |
| --- | --- |
| Brett Kelcey | 0170 |
| Frank Arrons | 0171 |
| Joanna Clark | 0172 |
| Martin Burns | 0173 |

**IT**

Manager: Alicia McKellips

Main Phone line: 415-555-8352

| Employees: | Phone Extension |
| --- | --- |
| Alicia McKellips | 0190 |
| Luke McDowel | 0191 |
| Allan Smith | 0192 |
| Joseph Webber | 0193 |
| Robert Wildhorn | 0194 |

## 

## Vendor Contact List

**Dell**

One Dell Way

Round Rock, Texas 78682

(1-800-WWW-DELL)

**HP**

3000 Hanover Street

Palo Alto, CA 94304-1185 USA

(800-282-6672)

**Bold Data Technology, Inc.**

dba BOLData Systems

48363 Fremont Blvd.

Fremont, CA 94538

800-923-2653

## Supplier Contact List

### Blank DVD/CD/Case Suppliers

**The Tech Geek – Primary Supplier**

48965 Warm Springs Blvd Fremont, CA 94539

Toll-Free: 1-800-456-0825

**Disc Makers – Secondary Supplier (In emergency)**

http://www.discmakers.com

7905 N. Route 130 Pennsauken, NJ 08110-1402

Toll-Free: 800-468-9353

Local: 856-663-9030

**Dub-It Media Services – Secondary Supplier (In emergency)**

Hollywood Sales Office

1110 North Tamarind Avenue Hollywood, California 90038

Toll-Free: 1-888-99DUB-IT

Local: 323-993-9570

**ISSI Business Solutions– Secondary Supplier (In emergency)**

22122 20th Ave SE #152 Bothell, WA 98021

Toll-Free: 1-800-660-3586

Local phone: 425-483-4801

### Box Suppliers

**Customized Packaging Solutions Inc. – Primary Supplier**

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

**The Packaging House, Inc. – Secondary Supplier (In emergency)**

6330 North Pulaski Road Chicago, Illinois 60646-4594

Toll-Free: 800-966-1808

**Ace Packaging of AZ– Secondary Supplier (In emergency)**

https://www.acepackagingaz.com/

4012 W Turney Ave #3 Phoenix, AZ 85019

Local: (602) 272-7231

### Paper Supplier

**JC Paper – Primary Supplier**

47422 Kato Rd Fremont, CA 94538

Local: (510) 413-4700

**Ace Packaging of AZ– Secondary Supplier (In emergency)**

https://www.acepackagingaz.com/

4012 W Turney Ave #3 Phoenix, AZ 85019

Local: (602) 272-7231

## Client Contact List

**Electronic Arts:**

209 Redwood Shores Parkway

Redwood City, CA 94065

**Ubisoft:**

625 Third Street

San Francisco - CA 94107

**Take-Two Interactive**

622 Broadway

New York, NY 10012

**LucasArts**

1110 Gorgas Avenue

San Francisco, CA 94129

**Nintendo**

Redmond, WA 98073

Capcom:

475 Oakmead Parkway

Sunnyvale CA, 94085

**Codemasters**

350 Fifth Avenue, 59th Floor

New York, NY 10118

**Midway:**

2704 West Roscoe Street

Chicago, IL 60618

**Activision**

3100 Ocean Park Boulevard

Santa Monica, California 90405

**THQ**

27001 Agoura Road Suite 325

Calabasas Hills, CA 91301

## 

## Product Distributors Contact List

### E.B Games - West Coast Stores

**EB Games #3302**

Broadway & Jackson

617 SW JACKSON ST

PORTLAND OR, 97201

503-221-8791

**Electronics Boutique #435**

Stoneridge

1384 STONERIDGE MALL

PLEASANTON CA, 94588 US

925-463-0932

**EB Games #667**

Arizona Mills

5000 ARIZONA MILLS CIR

TEMPE AZ, 85282

480-838-3958

**EB Games #401**

Fashion Show Mall

3200 LAS VEGAS BLVD. SOUTH

LAS VEGAS NV, 89109 US

702-731-1733

### Gamestop - East Coast Stores

#### 

**GameStop #872**

Westside Shopping Center

2477 Frederick Ave.

Baltimore MD, 21223 US

(410)945-3100

#### 

**GameStop #747**

Meadow Glen Mall (F)

3850 Mystic Valley Parkway

Medford MA, 02155 US

(781)395-3341

#### 

**GameStop #2201**

Coral Way

8743 SW 24th Street

Miami FL, 33165 US

(305)227-3795

### Wal-Mart - Nationwide Stores

#### 

**Wal-Mart Supercenter Store**

350 West Hope Avenue

Salt Lake City (C), UT 84115

(801) 484-7311

**Wal-Mart Store #2204**

1300 Des Plaines Avenue

Forest Park, IL 60130

(708) 771-2270

**Wal-Mart Store #1151**

6565 State Avenue

Kansas City, KS 66102

(913) 788-3331

## 

## 

## Company Resources

### Computer equipment

**Administrative Computers**

* + - Status: 10x Distributed
    - 10 x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad-Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10

**Sales Computers**

* + - Status: 9x Distributed, 3x Unused, 3x Local Database
    - 15 x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad-Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10

**Research and Development Computers**

* + - Status: In use when in demand
    - 3x Custom Computer Builds
      * Intel Core i7-4470
      * 32 GB of RAM
      * 4 TB SSD Hard Drive
      * NVIDIA GForce GTX 1660 Video Card
      * Gigabit Network Card
      * Dual 26 Inch Monitors
      * Windows 10 Professional

**Shipping Computers**

* + - Status: 4x Distributed
    - 4x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10

**Advertising Department Computers**

* + - Status: 5x Distributed
    - 5x Dell Optiplex 7010 Business Desktop Computers
      * Intel Quad Core i5-3470
      * 8GB of RAM
      * 500 GB SATA Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 17 Inch Monitor
      * Windows 10

**IT Department Computers and Servers**

* + - 5x Workstations
      * Intel Quad Core i7-4470
      * 16 GB of RAM
      * 1 TB SSD Hard Drive
      * Built-In Video Card
      * Gigabit Network Card
      * 21 Inch Monitor
      * Windows 10
    - 10x Servers
      * PowerEdge R620
      * 16 GB of RAM
      * 3 X 2 TB Hard Drive (configured to RAID 5)
      * Windows Server 2016
      * Dual Gigabit Network Cards
      * 15 Inch Monitor

**Manufacturing Computers**

* + - 10 x Custom Built Machinery Computer Systems

### Communication links

* + Dedicated High-Speed Fiber Internet commercial line
    - Dual OC3 Optical Lines
  + Building Network Category 5 Cable
  + Switches and Routers
  + Satellite
  + VoIP Phone Lines
  + Dedicated Phone Landline

### 

### Communications equipment

* + 10x Cisco Network Switches - Building Communications
  + Cisco Network Routers - Building Communications
  + VoIP Phones - Sales
  + Walkie-talkies - security
  + Cell Phones - (In Emergency)
  + Landline - Dedicated Emergency Services Phones
  + Fax Machine

### 

### Office equipment

* + 15 x Printers
  + Scanner
  + Photocopier
  + Paper Shredder

### 

### Office supplies

* + Blank DVD/CD/ Cases - For Producing Product - The Tech Geek
    - Disc Maker (In Emergency)
  + Box Suppliers - Packaging software- Customized Packaging Solutions Inc.
    - The Packaging House, Inc. (In Emergency)
  + Paper Supplier - For Box Inserts - JC Paper

### 

### Production Equipment

* + Number CD Stamping Machine
  + CD diagnostic Machine
  + High-Speed CD Manuals Printer
  + Shipping Conveyor Belt

## 

## Facility Access - Key Cards

| Building 1 Access | |
| --- | --- |
| Department | KEY ID |
| CEO | MASTER-1 |
| Administration | ADMN-1 / ADMN-6 |
| Sales | SLS-1 / SLS-9 |
| Purchasing | PUR1 / PUR-4 |
| Manufacturing | MNF-1 / MNF-6 |
| R&D | RD-1 / RD-5 |
| Security | SEC-1 / SEC-4 |
| IT | IT-1 / IT-5 |
| Maintenance | MNT-1 / MNT-6 |

## 

| Building 2 Access | |
| --- | --- |
| Department | KEY ID |
| CEO | MASTER-1 |
| Sales | SLS-1 / SLS-9 |
| Purchasing | PUR-1 / PUR4 |
| Shipping | SHP-1 / SHP-5 |
| Advertising | ADV-1 / ADV-6 |
| Manufacturing | MNF-1 / MNF-6 |
| R&D | RD-1 / RD-5 |
| Security | SEC-1 / SEC-4 |
| IT | IT-1 / IT-5 |
| Maintenance | MNT-1 / MNT-6 |

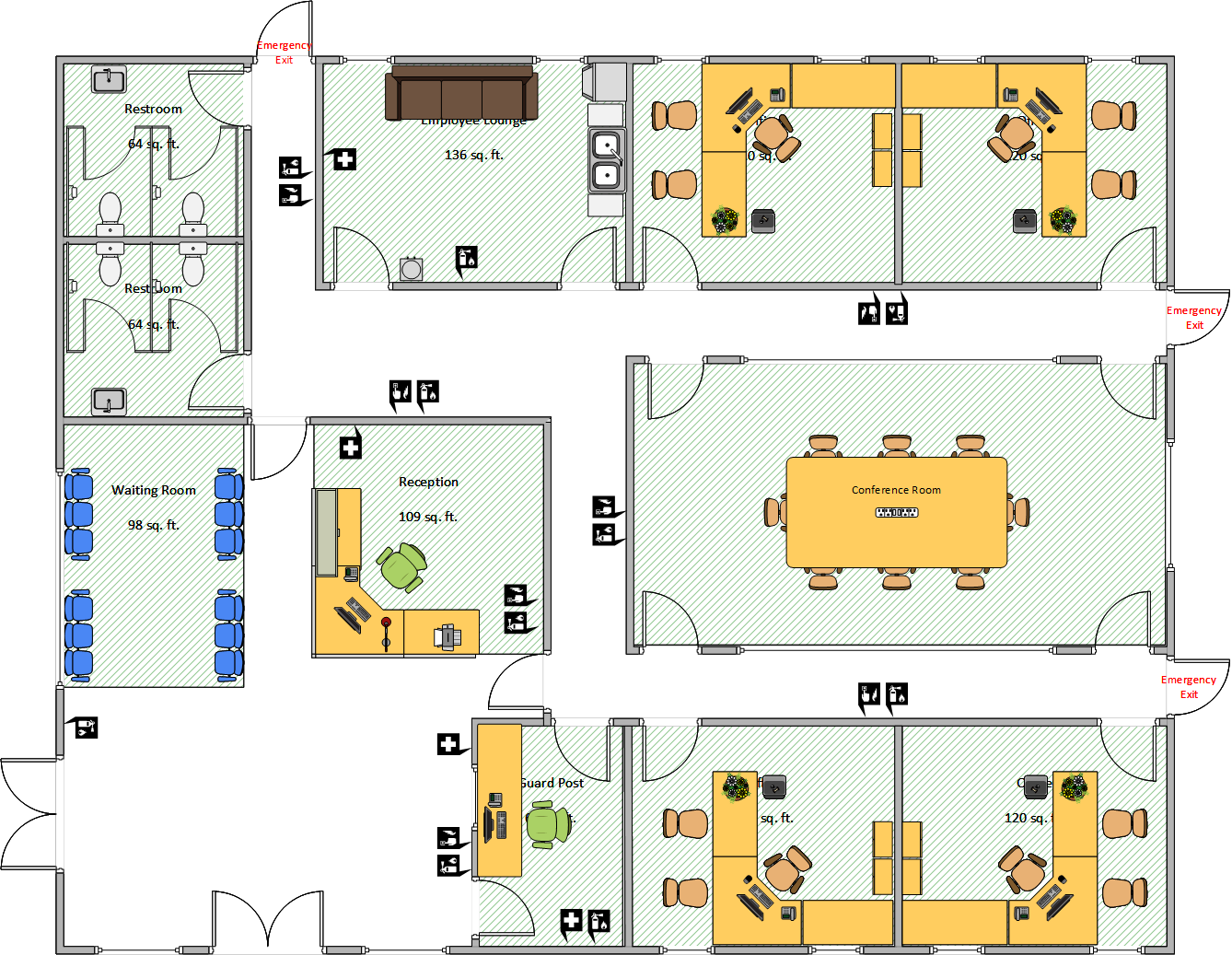
## 

| Building 3 Access | |
| --- | --- |
| Department | KEY ID |
| CEO | MASTER-1 |
| Shipping | SHP-1 / SHP-5 |
| Manufacturing | MNF-1 / MNF-6 |
| R&D | RD-1 / RD-5 |
| Security | SEC-1 / SEC-4 |
| IT | IT-1 / IT-5 |
| Maintenance | MNT-1 / MNT-6 |

## 

## Building Layouts

### Figure 1 - Building 1 internal layout



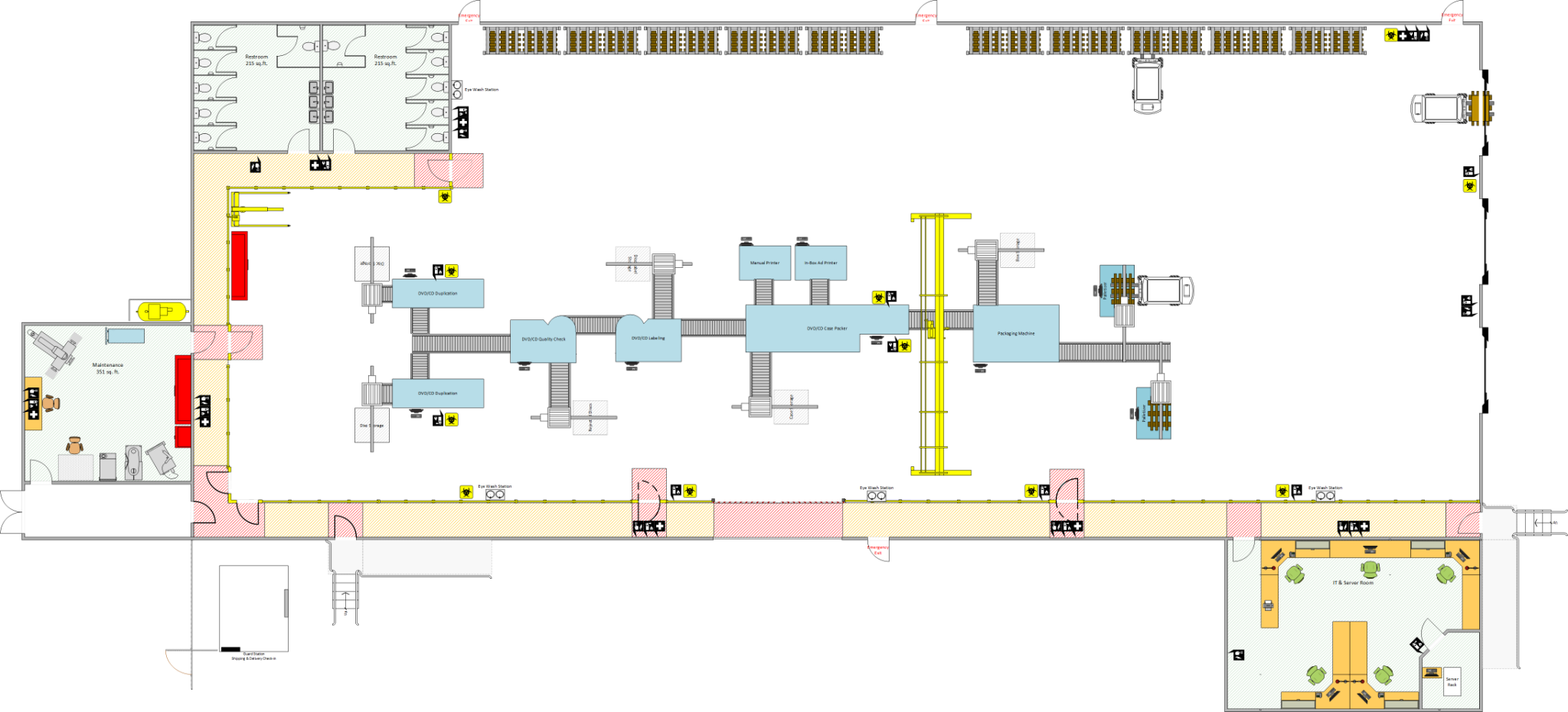
### Figure 2 - Building 2 level 1 internal layout



### Figure 3 - Building 2 level 2 internal layout



### Figure 4 - Building 3 internal layout



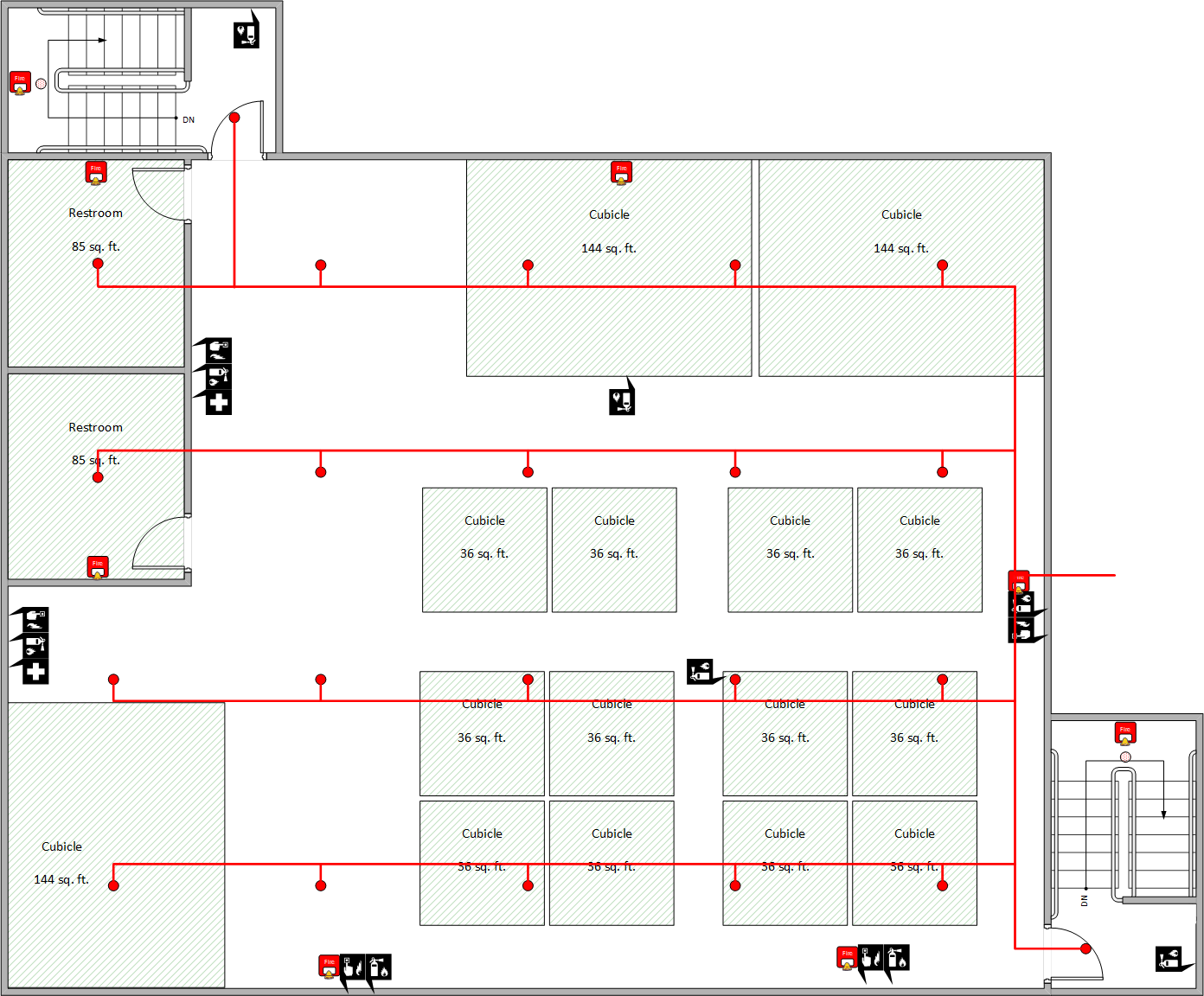
## Fire Suppression & Safety Equipment locations

### Figure 5 - Building 1

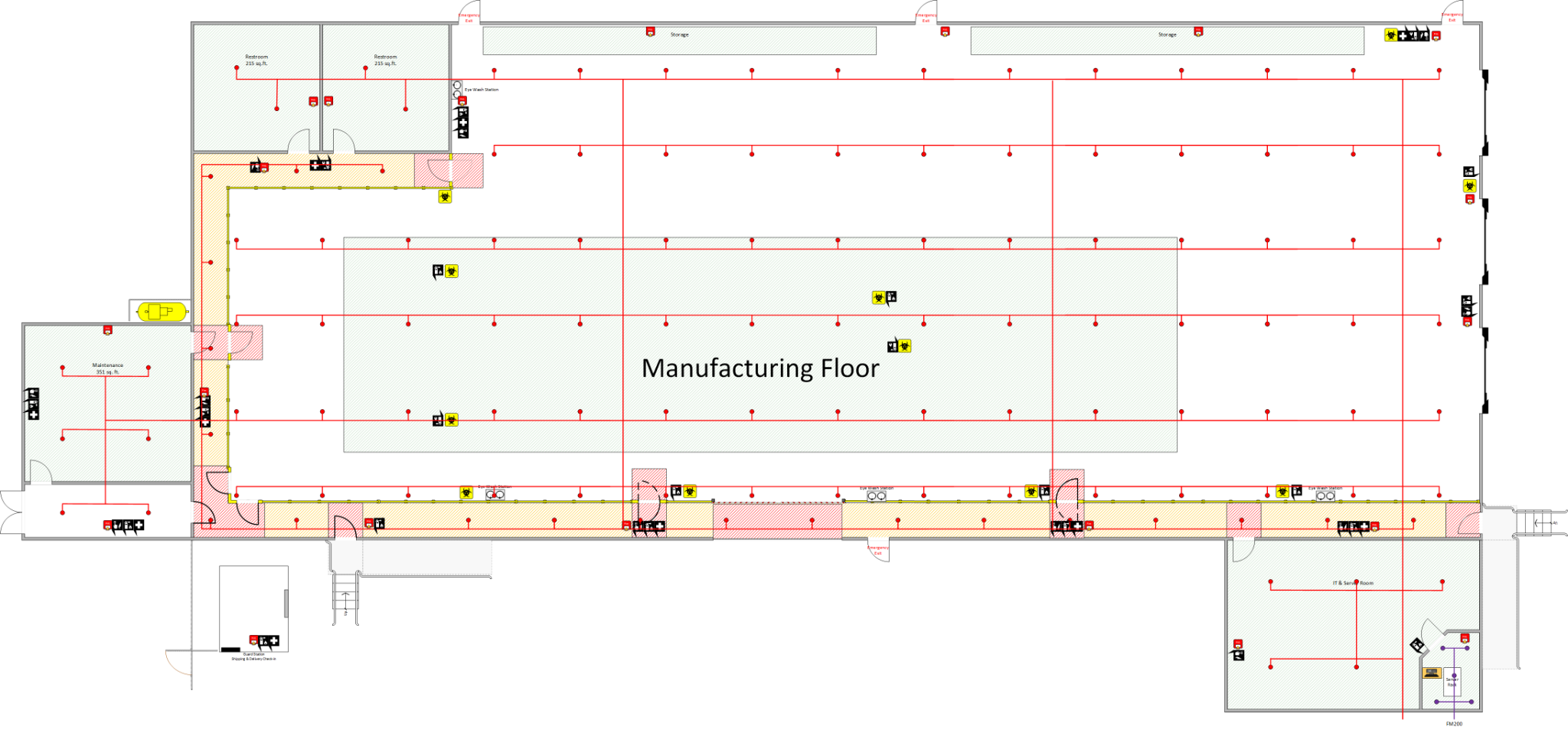
### Figure 6 - Building 2 level 1

### 

### Figure 7 - Building 2 level 2

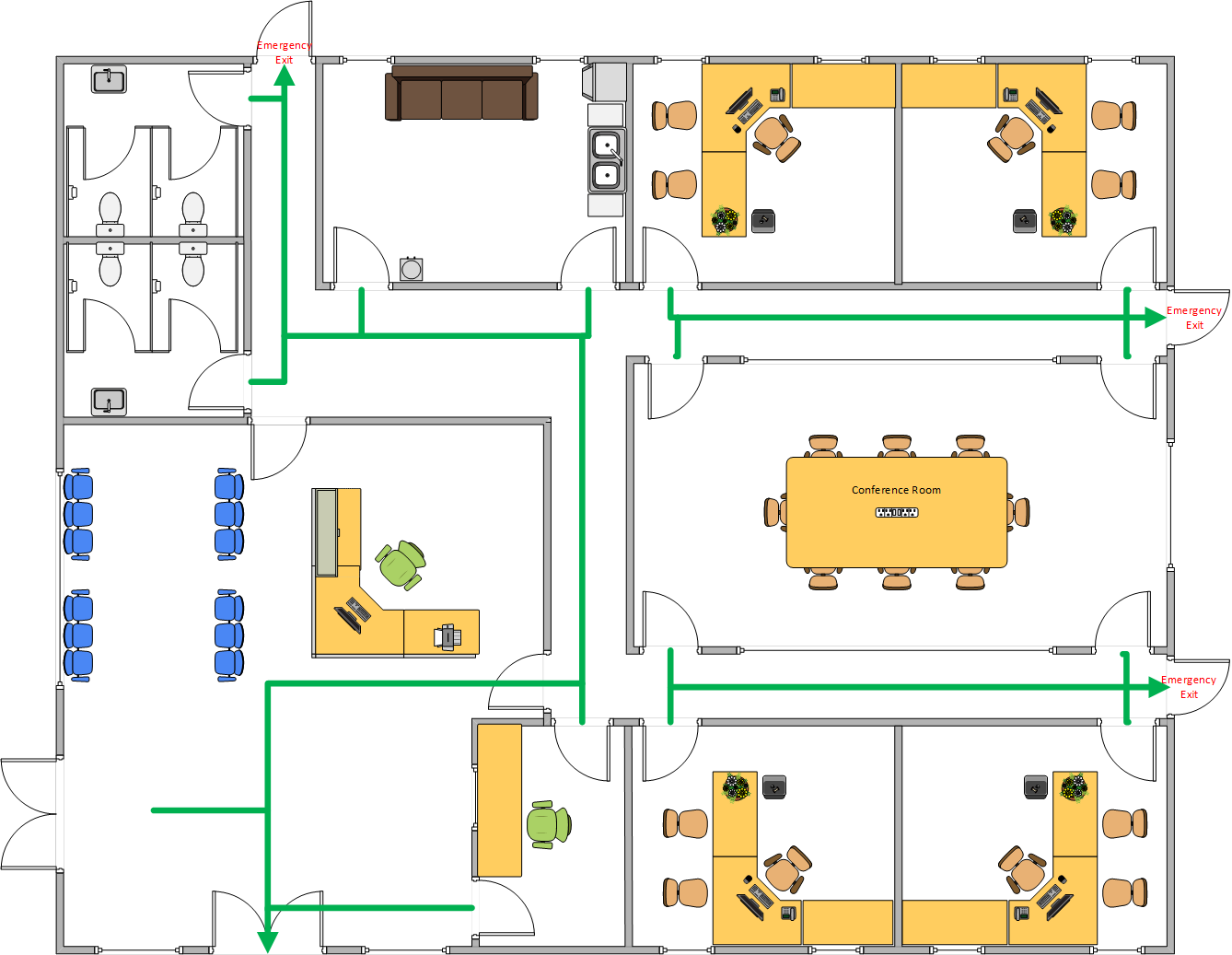


### Figure 8 -Building 3

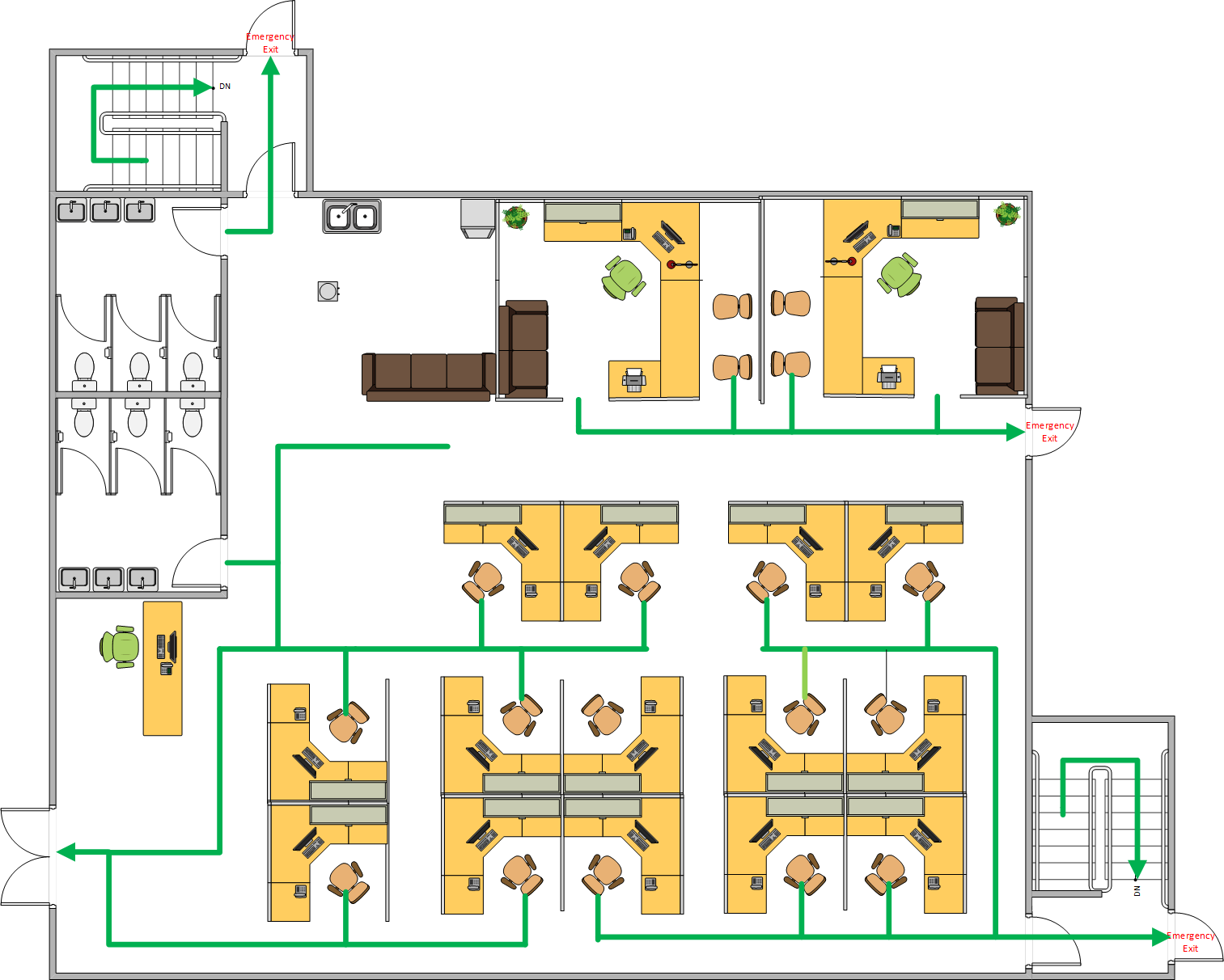


## Building Evacuation Maps

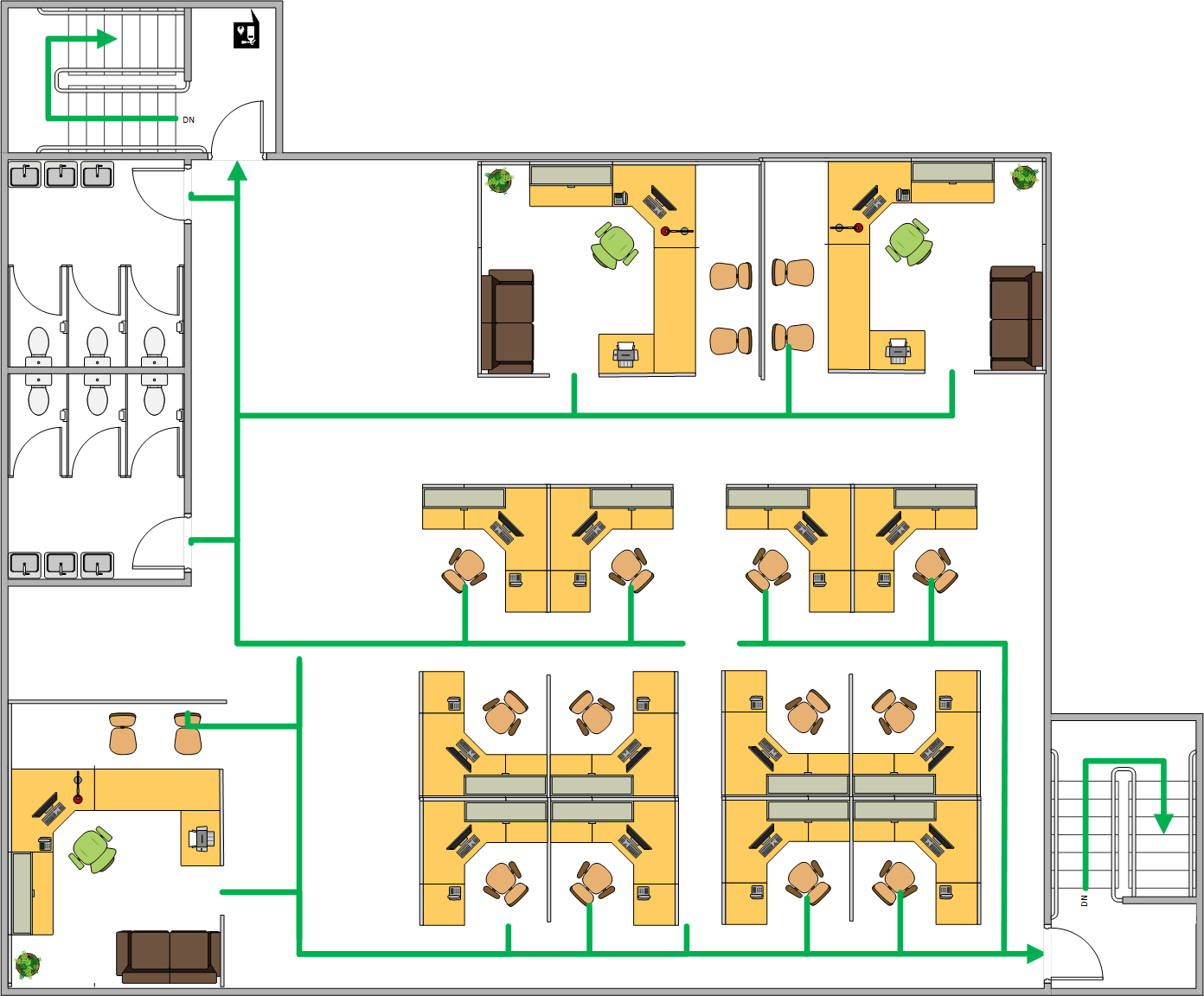
### Figure 9 - Building 1



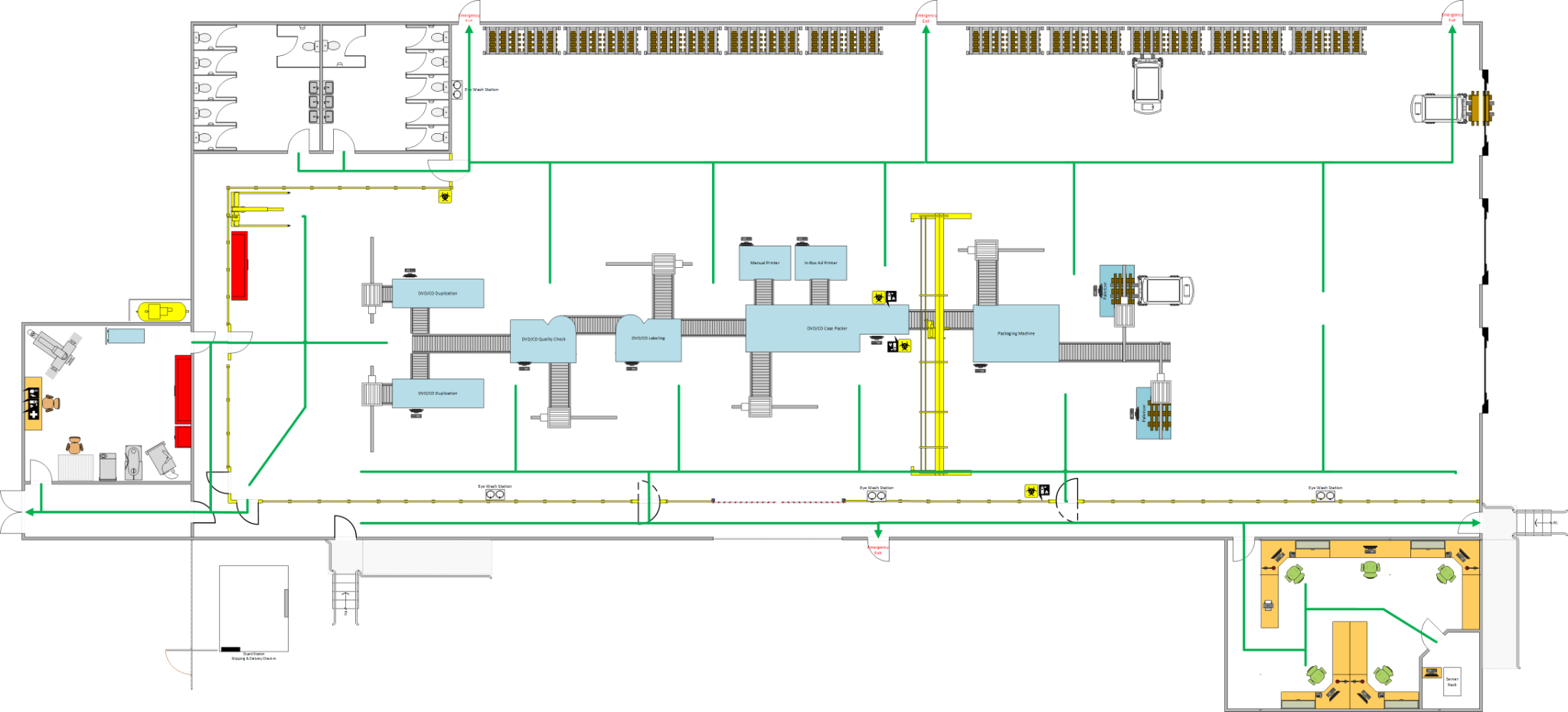
### Figure 10 - Building 2 Level 1



### Figure 11 - Building 2 Level 2



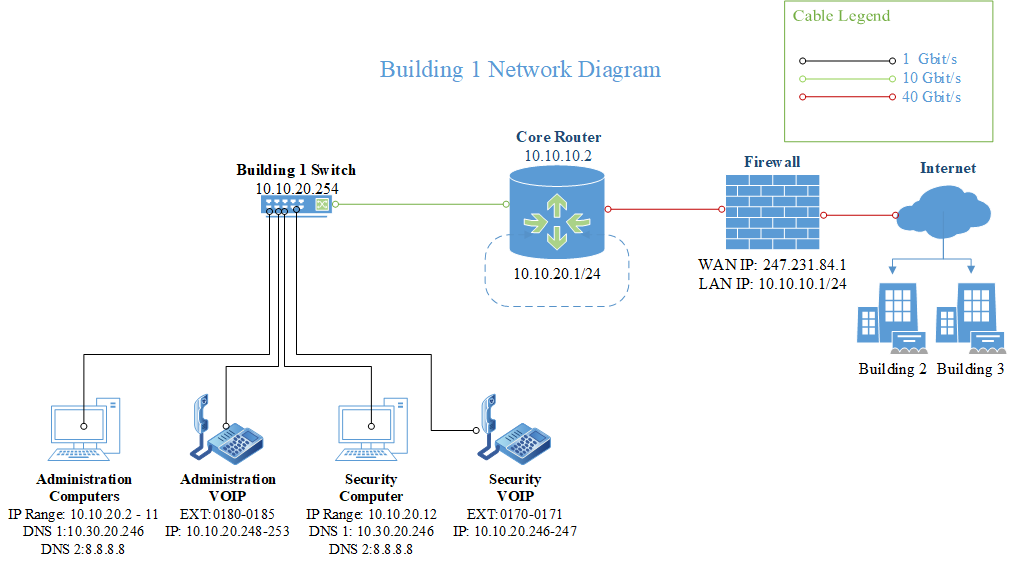
### Figure 12 - Building 3



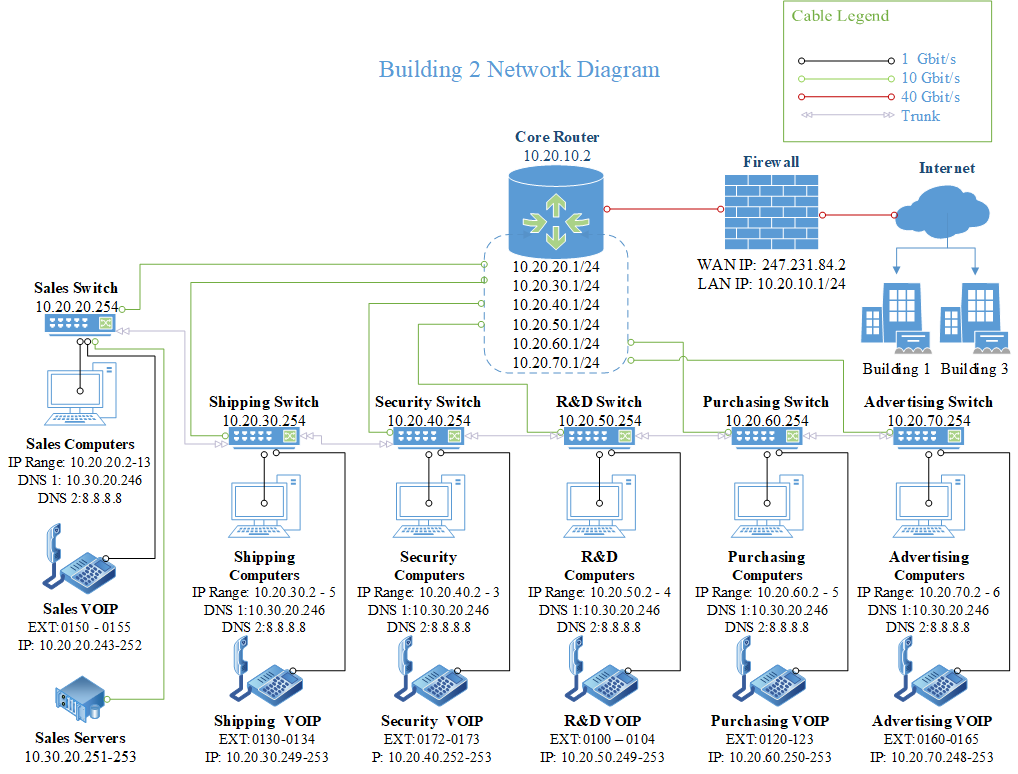
## 

## Network Diagrams

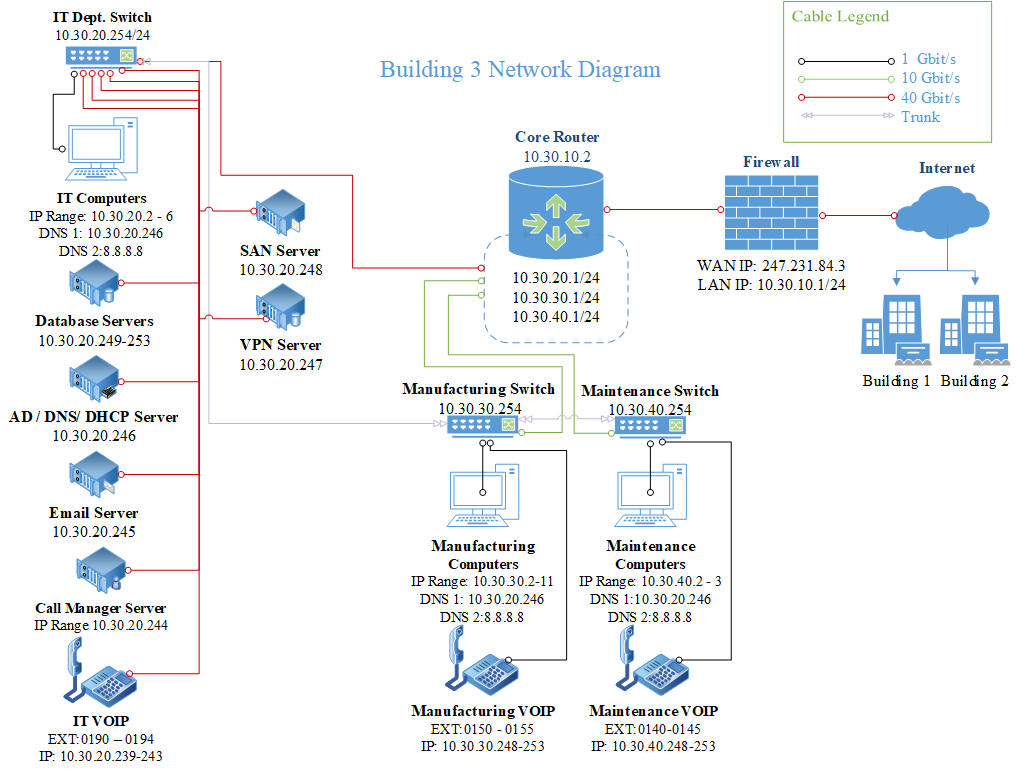
### Figure 13 - Building 1



### Figure 14 - Building 2



### Figure 15 - Building 3



## 

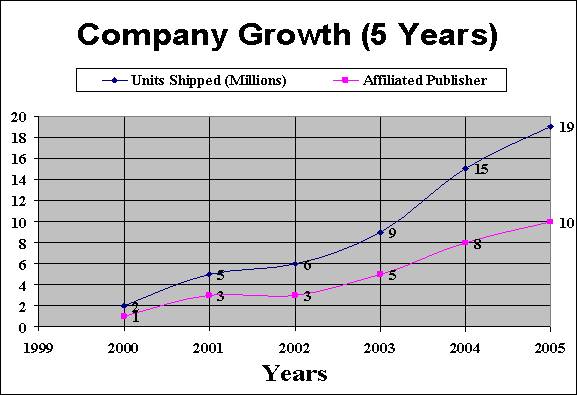
## Financial Statements

### Table 1 - Digiknights Financial Statement 2020

| Total Revenue | $200,000,000.00 |  |  |
| --- | --- | --- | --- |
| Less Staff Salaries and Benefits | ($6,900,000.00) |  |  |
| Less Operational Costs\* | ($125,000,000.00) |  |  |
| Net Profit | $68,100,000.00 |  |  |
| Operational Costs include supplies, materials, maintenance, contracts, insurance, rent, vehicles, etc | | | |
| **Revenue By Customer** |  | Units | Cost Per |
| Electronic Arts | $65,000,000.00 | 2600000 | 25 |
| Ubisoft | $5,000,000.00 | 125000 | 40 |
| Take-Two Interactive | $2,000,000.00 | 50000 | 40 |
| LucasArts | $40,000,000.00 | 1333333.333 | 30 |
| Nintendo | $50,000,000.00 | 1666666.667 | 30 |
| Capcom | $4,000,000.00 | 100000 | 40 |
| Codemasters | $7,000,000.00 | 189189.1892 | 37 |
| Midway | $6,000,000.00 | 162162.1622 | 37 |
| Activision | $20,000,000.00 | 571428.5714 | 35 |
| THQ | $1,000,000.00 | 25000 | 40 |
| **Total** | **$200,000,000.00** | 6822779.923 |  |
|  | Monthly | 568564.9936 |  |
|  | Weekly | 136455.5985 |  |
|  | 5 Production Machines | 27000 units each week per machine | |

## Company Growth

### Figure 16 - Company Growth (5 Years)



## Organizational Chart

## 

## 

## Assessment Forms

## Form 1 - Initial Asset Inventory and Assessment

Inspection Date: Inspector Name:

Building Number: Room

|  | Damage | | | |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Asset Name | Unknown | Minor | Moderate | Severe | Repairable | Value | Downtime | Comments/ Cause of Damage |
|  |  |  |  |  | * Yes * No |  |  |  |
|  |  |  |  |  | * Yes * No |  |  |  |
|  |  |  |  |  | * Yes * No |  |  |  |
|  |  |  |  |  | * Yes * No |  |  |  |
|  |  |  |  |  | * Yes * No |  |  |  |
|  |  |  |  |  | * Yes * No |  |  |  |
|  |  |  |  |  | * Yes * No |  |  |  |
|  |  |  |  |  | * Yes * No |  |  |  |

# 

### Form 2- Building Damage Assessment

Inspection Date: Inspector Name:

Building Number: Room:

| Space is (Check all that apply) | | | | |
| --- | --- | --- | --- | --- |
| * Not Usable | * Usable | * Wet | * Damp | * Dry |
| Utilities are operational (Check all that apply) | | | | |
| * Phone | * Internet | * Power | * Water | * Sewage |
| Ceiling tiles (e.g. wet, sagging, missing) | | | | |
| Walls (e.g. cracks, watermarks, soot) | | | | |
| Floor/Carpet (e.g. wet, burnt, torn, mildew) | | | | |
| Water leaks (e.g. from roof, through walls, windows) | | | | |
| Doors/Windows (e.g. broken locks, hinges, awnings) | | | | |
| Fixtures (e.g. electrical outlets, lighting) | | | | |
| Other | | | | |
| Comments | | | | |

### Form 3 -Individual Asset Assessment

Inspection Date: Inspector Name:

Building Number: Room: Department:

Asset Description Model # Inv ID #

Contract #

Overall Damage: Unknown Minor Moderate Severe **Total loss**

Asset Repairable: Yes No

Estimated Repair/Replacement Cost

Estimated Downtime

| Describe Visual Condition: (e.g soot, wet, crushed, tipped over) | | | | | |
| --- | --- | --- | --- | --- | --- |
| List Components | | | | | |
| Usable | | Repairable | | Replace | |
| Name | Value | Name | Cost | Name | Cost |
|  |  |  |  |  |  |
| Comments | | | | | |

# 