IT Statement of Intent

This document outlines our policies and recovery procedures after an IT disaster. A disaster is defined as any event that would cause data loss or loss of control of data from any of our medical offices. This document should be updated and modified to keep our people and systems safe. Fountain Valley Medical’s (FVM) IT mission is to ensure information systems uptime, data integrity, and availability.

Policy Statement

The Doctors, Nurse Practitioners, and office managers have approved the following policy statement.

1. FVM will develop a comprehensive IT disaster recovery plan
2. A formal risk assessment will be completed to determine the requirements for the disaster recovery plan.
3. The disaster recovery plan should cover all essential and critical infrastructure elements, systems, and networks by business activities.
4. The disaster recovery plan should be tested every six months in a simulated environment to ensure its ability to be implemented in emergency situations.
5. All staff must be trained on the disaster recovery plan and their respective roles. These roles will be tested during a simulation.
6. The disaster recovery plan should be updated regularly to track changes in the company.

Objectives

Disaster Contact list

| Name / Title | Contact options | Contact information |
| --- | --- | --- |
| Betty Thorn - Office manager | Home | (xxx)xxx-xxxx |
|  | Work number | (xxx)xxx-xxxx |
|  | Email | b.thorne@fountainvalleymedical.com |
|  |  |  |
| Bob Farland - office manager | Home | (xxx)xxx-xxxx |
|  | Work number | (xxx)xxx-xxxx |
|  | Email | b.james@fountainvalleymedical.com |
|  |  |  |
| Jordan Huff - Tier 2 tech support | Home | (xxx)xxx-xxxx |
|  | Work number | (xxx)xxx-xxxx |
|  | Email | j.huff@fountainvalleymedical.com |
|  |  |  |
| Jamie Stroble - IT Director | Home | (xxx)xxx-xxxx |
|  | Work number | (xxx)xxx-xxxx |
|  | Email | ja.stroble@fountainvalleymedical.com |

External contacts

| Name / Title | Contact Options | Contact information |
| --- | --- | --- |
| **Property Management** | Office Number | (xxx)xxx-xxxx |
| Fountain Valley Property Management Group | Emergency after hours | (800)xxx-xxxx |
|  |  |  |
| **Power Company** | Office | (800)xxx-xxxx |
| Indiana Power and Light |  |  |
|  |  |  |
| **VOIP Service** | Office | (800)xxx-xxxx |
| Zac Darnell | email | zac@indyvoip.tech |
|  |  |  |
| **Insurance** | Office | (800)xxx-xxxx |
| AC# 12345678AES | National number | (800)xxx-xxxx |
|  |  |  |
|  |  |  |

**Plan updating**

The disaster recovery plan must be updated as the company’s processes and procedures change. Changes should be appropriately updated through the IT Director. The plan should be thoroughly tested, and appropriate amendments should be made to the training materials. Additional testing days and environments may be added after an update at the IT director and owner’s discretion.

**Documentation Storage**

Copies of the plan (flash drive, complex companies) will be stored in a secure location to be defined by the owner. Each member of the senior management (Doctors, Nurse Practitioners, Office managers) will be issued a hard copy and a virtual copy in their private folders. Each disaster recovery team member will be issued a hard copy and access to virtual copies on their machines.

Backup Strategy

Key business processes and agreed backup strategies are defined and listed below. The strategy chosen is an AWS SQL and file server; the backup process will involve AWS lambda scheduled differential backup of SQL server along with a nightly backup of files after business hours.

| Business Process | Backup strategy |
| --- | --- |
| Tech - Hardware | Here is a list of all physical assets, serial numbers, and locations. I have two desktop PCs and two laptops as backups in a secure offsite location. |
| Tech - Software | Image of laptops and desktops kept in the IT office. Office software is on a backup folder at local servers in each office and on a hard drive kept offsite. |
| Electronic Health Record | Database backup on AWS cloud 3-hour backups to keep AWS costs down. |
| Patient Documentation | Nightly backup on AWS file server |
| Email | Nightly backup on AWS file server |
| Payroll | Weekly backup on AWS file server |
| Office Documentation | Nightly backup on AWS file server |
| Website | 3rd party hosted |
| Test environment | An image of the test environment was saved in the tech office, and a copy was saved offsite and updated as needed. |

**Risk Management**

Many potential disruptive threats can occur at any time and affect business operations. We have considered many potential threats, and the results are listed below. Each potential disaster has been examined and ranked.

Probability 1=very high, 5 very low - Impact 1=total destruction, 5 minor annoyance

| Potential Disaster | Probability Rating | Impact rating | description |
| --- | --- | --- | --- |
| Flood | 5 | 4 | The office is on the second floor of a building in a low flood-risk zone. First-floor circuits blowing could cause damage to hardware |
| Fire | 3 | 3 | A fire suppression system was installed in the server room. Smoke and fire detectors in each room of the office. |
| Tornado | 5 |  |  |
| Act of terrorism | 5 | 4 |  |
| Act of Sabotage/theft | 4 | 5 | The server room is to remain locked at the location. GPS tracking of portable equipment should remain enabled. Theft tracking by serial number and use plus use of cameras by exits to limit theft/sabotage |
| Electronic power failure | 3 | 4 | Redundant UPS array with remote monitoring |
| Loss of communications network service | 4 | 4 | Two diversly routed t1 trunks into the building. Wan redundancy. |

Emergency

**Emergency Alert**

The person discovering the incident calls a member of the ERT, as listed below.

Once contact has been made, the person who discovered the incident does not need to make further calls.

1. Office Manager
2. IT tier 2
3. IT director
4. FVM Owner

**Activation of emergency response team**

When an incident occurs, the emergency response team (ERT) must be activated. The ERT will then decide the extent to which to invoke the Disaster recovery plan.

1. Respond immediately to the potential disaster and call emergency services if needed.
2. Assess the extent of the disaster and its impact on the business.
3. Decide which elements of the DRP should be activated
4. Establish and manage a disaster recovery team to maintain vital services and return to normal operation
5. Ensure employees are notified and allocate responsibilities and activities as required

**Disaster Recovery team**

The team will be contacted and assembled by the ERT. The team’s responsibilities include

1. Establish facilities for an emergency level of service within two business hours.
2. Restore key services within four business hours of the incident
3. Recover to business as usual within 24 hours after the incident
4. Coordinate activities with the disaster recovery team, first responders, and emergency personnel as needed
5. Report to the emergency response team

**Procedures for management**

Office managers and Nurse practitioners will keep a hard copy of each employee in their office. In addition, office managers will have a hard copy of the FVM disaster recovery and business continuity plans on file in their homes if the office building is inaccessible.

**Assessments**

The ERT shall prepare an initial assessment of the impact of the incident and its impact on FVM.

1. Loss of patient personal identifying information
2. Loss of financial documents
3. Loss of hardware and software
4. Theft of hardware or information

**Legal action**

The FVM legal department and ERT will jointly review the incident’s aftermath to decide whether legal actions may result from it. In particular, claims by or against the company for regulatory violations are possible.

Templates disaster recovery plan

| System | Location | information |
| --- | --- | --- |
| Production server SQL | Headquarters Corpus Christie Avenue | Server: XXXX  CPU: XXXX IP: XX.XX.XX.XX  Serial no: XXXXXXXXXXX |
| backup | AWS |  |
|  |  |  |
| File Server | Headquarters Corpus Christie Ave | Server: XXXX  CPU: XXXX IP: XX.XX.XX.XX  Serial no: XXXXXXXXXXX |
| Backup | AWS |  |
|  |  |  |
| Email server | 3rd party web host | Contact info: xxxxxxx |
| backup | AWS |  |
|  |  |  |
| Internet | Local OFFICE server room | The office manager has a code for the door |
|  |  |  |