**Prepared by: Mohammad Fahim Nazari**

**Facility Pro Disaster recovery solution**

**Overview of the plan**

The disaster recovery plan outlines the strategies and responsibility for the Facility Pro on AWS cloud-based architecture in the event of disaster. The plan considers various potential thread such physical, system failure, cyber security attack and telecommunication failure. This plan provides the mitigation and risk presentation and back up strategy.

**Identified risk for Facility Pro**

Some of the common risk that associated with the premises infrastructure for the business could be the following.

* Human error leading to data loss.
* Cyberattack leading to system compromise.
* Natural disaster damaging data centre.

**Facility Pro Preventative Plan**

* Using the least privilege policy.
* Using multiple availability zone deployment
* Regular patching and update
* Implementing strong security group policies
* Using AWS shield for DDoS protection.

For the physical security AWS data centres have extensive physical security measures in place. For the system failure we can use regular checks and automated failover. In case of Attach we used DDoS protection to keep our system safe.

## **Preparation for disaster recovery for Facility Pro**

We know that AWS allows us to spread our services across multiple regions and availability zones for redundancy. The backup strategy for facility pro will be handled regularly and automated backups and the ability to quickly restore these backups in a different region if necessary. In the event of disaster, we have set up an AWS multi-AZ deployment for redundancy, implement automated backups for data. And now we must create a disaster recovery team to handle the disaster.

## **Key Personnel**

The key personnel will include the CIO, IT Manager, and all members of the disaster recovery team.

## **A step by step of Facility Pro disaster Recovery**

* Detection and assessment of the disaster (within 20 minutes)
* Activation of the disaster recovery team (within 30 minutes)
* Implementation of disaster recovery procedures (within 45 mins)
* Verification of recovery and testing (within 1 hours)
* Return to normal operations (within 1.35 hours)
* Mean Time to Repair (MTTR)
* Our goal is to have an MTTR of less than 1.3 hours to meet our RTO.