**Prepared by: Mohammad Fahim Nazari**

**Facility Pro disaster recovery plan**

As the company concern about cyber threats and failure of the architecture design for potential loss of data I prepared a disaster recovery plan to make sure to avoid the incident and provide the mitigation and recovery plan if an accident happens.

**Facility Pro’s disaster recovery policies and procedure:** Facility Pro has a well-documented disaster and recovery policies and procedure which will be updated and reviewed as necessary. The policies outlined a clear role, responsibilities, communication and over disaster recovery plan.

**AWS services provide for disaster and recovery plan.**: According to the policies and procedure of the Facility pro AWS cloud provide services to cover disaster recovery plan to avoid any loss of data. It’s important to understand the RTO and RPO while choosing to implement our plan for disaster recovery plan.

* Two VPC: having multiple VPC in different availability zone will help provide redundancy and fault tolerance.
* Disaster Recovery Procedures: A well-documented disaster recovery plan which shows step by step procedure such as AZ failure and region wide disruption.
* Cross Region Replication: if storing data in s3 buckets applying cross region replication will help quick data recovery in case of region failure.
* Incident response communication: provide a clear communication channel in case of escalation procedure and action response.

**Security levels for data management**: Facility Pro assessing the security level of data management to make sure the sensitive user data is protected. AWS provide different mechanism to provide data protection some are as follow.

* Data encryption: AWS provide several encryption mechanisms to protect user data such as KMS.
* Identity and Access Management (IAM): allow you to manage user permission.
* Network security: On the VPC level.
* DDoS: AWS shield provide protection against distributed denial of service attacks.

**Risk analyses of resources:** Facility pro risk analyses of resources will be conducted to identify potential risk into the company resources. The potential could be natural disaster, human error, or cybersecurity attack. AWS cloud can help the company with the following services to take care of the risk for the company.

* AWS CloudTrail: It provide record of the API within your account that help you get insight into resources changes or unauthorized access attempts for potential risk.
* AWS CloudFormation: It help during the deployment of resource with configuration and reduce risk to the resources.
* AWS trusted advisor: provide real time guidance to optimise your AWS infrastructure.
* AWS config: Enable you to take control of you resource configuration.

**Evaluation and Financial impact of loss and severity of Risk**: It is very important to understand the severity of an event happen for the business, the down time, data loss and damage that it can have on the company. The down time may cost the company financial loss and the company reputation. Loss of data may impact the company that the company loss reputation and get sued and that may have some serious consequences.

The disaster recovery plan will utilize the architecture design of two instances in two availability zones with load balancing and auto scaling to ensure redundancy and high availability. It will leverage AWS's built-in disaster recovery features and services, along with additional measures tailored to Facility Pro's specific requirements and risk profile. The plan will address various scenarios, including infrastructure failures, data loss, and service disruptions, to minimize downtime, protect data integrity, and enable swift recovery. Regular testing, maintenance, and ongoing review of the plan will be conducted to ensure its effectiveness and alignment with the evolving business needs.