Disaster Recovery Plan for BiteDance

# 1. Introduction

This document outlines the disaster recovery plan for the Heineken Vietnam application, ensuring business continuity in the event of a disruption.

# 2. Application Overview

- Front-End (DMZ): Web app using React and HTML hosted on a VM.

- Back-End (Green): .NET application with Business, Data, and Service layers.

- Database: SQL Server and SharePoint List.

- Services:

- Azure Communication Service

- Microsoft Entra ID

- Azure VM

# 3. Objectives

- Minimize downtime and data loss.

- Ensure rapid restoration of services.

- Maintain communication with all stakeholders during a disaster.

# 4. Risk Assessment

- Network Failure: Loss of internet connectivity.

- Hardware Failure: VM or server malfunction.

- Data Corruption: Database corruption or loss.

- Security Breach: Unauthorized access or data breach.

# 5. Disaster Recovery Strategies

## 5.1. Network Failure

- Mitigation: Use redundant internet connections.

- Recovery: Switch to backup ISP if primary fails.

## 5.2. Hardware Failure

- Mitigation: Regular maintenance and monitoring.

- Recovery: Use Azure VM snapshots for quick restoration.

## 5.3. Data Corruption

- Mitigation: Regular backups of SQL Server and SharePoint List.

- Recovery: Restore from the latest backup.

## 5.4. Security Breach

- Mitigation: Implement strict IAM policies with Microsoft Entra ID.

- Recovery: Revoke compromised credentials and restore data from secure backups.

# 6. Backup Procedures

- SQL Server: Daily full backups and transaction log backups every 4 hours.

- SharePoint List: Weekly exports.

- Azure VM Snapshots: Taken weekly.

# 7. Recovery Procedures

## 7.1. Front-End Recovery

- Deploy latest React app build to a new VM if necessary.

- Ensure OBS and firewall configurations are restored.

## 7.2. Back-End Recovery

- Restore .NET application from the latest build.

- Reconfigure API settings and firewall rules.

## 7.3. Database Recovery

- Restore SQL Server from the latest backup.

- Verify SharePoint List data integrity.

# 8. Communication Plan

- Internal Team: Immediate notification via email and messaging apps.

- Clients: Inform via email and website notification.

- Updates: Regular status updates every hour until resolution.

# 9. Testing and Maintenance

- Testing: Conduct quarterly disaster recovery drills.

- Maintenance: Regularly update and review the disaster recovery plan.

# 10. Roles and Responsibilities

- Disaster Recovery Lead: Coordinates recovery efforts.

- IT Support Team: Executes recovery procedures.

- Communications Manager: Manages stakeholder communication.

# 11. Conclusion

This disaster recovery plan is designed to ensure the BiteDance application remains resilient and can recover swiftly from any disruptions. Regular updates and testing will be conducted to maintain its effectiveness.