Disaster Recovery Plan

Contents

Purpose

The Disaster Recovery Plan is an outline of the detailed steps required to restore the AWS Infrastructure – systems, applications, and services in the event of a disaster.

RPO, RTO, WRT, and MTD objectives:

1: Recovery Point Objective(RPO): 5min The maximum sustainable data loss based on backup schedules and data needs.
2: Recovery Time Objective (RTO): 3 hours The duration of time required to bring critical systems back online.
3: Work Recovery Time (WRT): 1 hour The period needed to recover lost data (based on RPO) and to enter data resulting from work backlogs (manual data generated during system outage that must be entered):
4: Maximum Tolerable Downtime (MTD): 4 hours The duration of the RTO plus the WRT.

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app

System Overview	
Application Description	MENU is a digital self-order & pay ecosystem consisting of mobile, terminal and web-Apps to enable guests to order & pay from different devices, so as • to reduce waiting times and lines, • to generate more orders & re-orders, and • to reduce service complexity.
Platform	AWS
Technology	Laravel PHP, RDS MySQL Database, and ElastiCache Redis, Elastic Beanstalk, EC2, S3, CloudFront
Recovery Strategy	Pilot Light environment configuration on the second, backup AWS Ireland Region
Assumptions	All Data and Operations successfully recovered from the main, primary AWS Frankfurt- EU, AWS Virginia – US, and AWS Sao Paolo – US to the second, backup AWS Ireland Region

DR Plan Name	MENU Application DR Plan
DR Plan Owner and Maintained By	Name: Aleksandar Nenov Title: AWS Infrastructure Manager / System Administrator Phone Number: +38166398398 E-Mail: aleksandar@menu.app

Disaster Recovery (DR) Plan Maintenance Procedures

The procedures for maintaining this Disaster Recovery Plan are:

- **Review Cycle** – The DR Analysts do a periodic review with the DR Plan owner to ensure the accuracy of the DR Plan.
- **Review Configuration Changes** – This Plan will be reviewed and updated as required when there is any change to a system, application, network connection or security mechanism configuration of the system or application or service for which this DR Plan is developed.
- **Making Suggestions For Changes To The DR Plan** – All IT staff are encouraged to provide suggestions and recommendations to the DR Team Leader for consideration
- **DR Plan Approval Process** – This DR Plan must be approved by those listed in Annex C, DR Plan Approvals.
- **Applications Included in This Disaster Recovery Plan**

Application Name	Application Components	Department
MENU EU (main)	API EU – https://api.menu.app	IT
	CMS EU – https://cms.menu.app	IT
	KIOSK EU - https://kiosk.menu.app	IT
	CLIENTS EU - clients.menu.app:9000	IT
MENU US	API US – https://api-us.menu.app	IT
	CMS US – https://cms-us.menu.app	IT
	KIOSK US - https://kiosk-us.menu.app	IT
	CLIENTS US – clients-us.menu.app:9000	IT
MENU LAC	API LAC – https://api-lac.menu.app	IT
	CMS LAC – https://cms-lac.menu.app	IT
	KIOSK LAC - https://kiosk-lac.menu.app	IT
	CLIENTS LAC - clients-lac.menu.app:9000	IT
		IT
MENU Website	https://menu.app	IT

Recovery Procedures and Checklists

Once directed to do so the DR Team will begin to recover the disrupted or damaged IT system or service following:

- The recovery process contained in this DR Plan

1 - Use of Pilot Light Resources

The IT Operations Team Leader will ensure that the IT systems or services have failed over correctly to the pilot light site and is operating successfully from the Pilot Light back up using the backup configuration.

#	Item	Details
1	Description of Backup / Failover Capability	All data and configuration are saved via Backup and replication procedure to the second, backup AWS Ireland site.
2	Description of how the backup/failover capability is activated	The Failover capability is activate once all DNS records are pointed to the second, backup site.
3	How to Determine that the backup/failover capability has worked properly	By checking that the replicated database is promoted to the primary one and the Elastic Beanstalk app has been connected properly to the database and reconfigured to used replicated S3 data, and by checking all network AWS VPC configurations.
4	Once the failed system has been recovered, how the system will be returned to the main site from the backup/failover site	By recreating a new primary RDS MySQL database from to the second, backup database which has been promoted as a new primary (read-write) on the main primary MENU EU/US/LAC site and by recreating the primary S3 storage from the activated replica on the second backup AWS Ireland site.

2 - Application Restoration

The Team will recover the systems, applications or services as follows:

#	Description	Specific tasks
1	Rebuild or replace non-functioning AWS services and software:	**Application Recovery** Configure latest ElasticBeanstalk app configurations on the second, backup AWS Ireland Region. **Database Server Recovery** Promote the RDS Read Replica as the primary one and reconfigure the EB to use it inline with the new ElastiCache configuration, if S3 and Cloudfront endpoints are affected
2	Reload all required software and data	**Application Recovery** Deploy latest ElasticBeanstalk app version on the second, backup AWS Ireland Region.

#	STEP	SPECIFIC TASKS
1	Verify network connectivity – check all network connections (VPCs, Subnets IP gateways, and addressing)	Check VPC, Subnets IP gateways, and addressing
2	Verify security mechanisms, settings, and configuration	Security Groups, access control mechanisms – IAM accounts and roles privileges
3	Connect IT or service to the network	After doing STEP 1 and 2 above the new second, the backup system will be connected to the network.
4	Perform operational test over the network to ensure that IT system, application or service works correctly over the network	Test application functionality on the new second, backup site, after DNS switch.

3 – Reconfigure and Reconnect

Once the systems, applications or services have been recovered, tested and is working correctly, the systems, applications or services will next be reconnected to the network.

4 – Operational Testing

Once the systems, applications or services have been reconnected to the network, the Team will perform the following tests to confirm that the systems, applications or services are operating correctly.

#	STEP	SPECIFIC TASKS
1	Test the IT system, application or service to ensure proper operation	Test all endpoints URL and functionality
2	Test all interdependencies with other systems, applications, and services to ensure that interdependencies work correctly	Check new configurations parameters and services configurations
3	Test end-user connection over the network to test the recovered systems, applications or services.	Check all application components as an end-user