BUSINESS CONTINUITY PLAN - IT
(Disaster Recovery Plan)

QHP803

1. Introduction

National Ambulance's business continuity strategy provides an overarching framework for the development and implementation of business continuity plans, specific to an area of risk or operations identified through the business continuity risk assessment. The individual business continuity plans are developed according to requirements of the NCEMA 7000:2015 standard.

2. Purpose

The aim of this plan is to address the risks identified in National Ambulance's (NA's) business continuity risk assessment relating to IT Operations.

3. Scope

This plan includes the main steps required to trigger, implement and recover back from IT Disaster Recovery (DR) for National Ambulance Head Office services.

It does not include DR plans for service providers other than where connections to those service providers enters the National Ambulance Head Office.

4. Key Obligations and References

IT DR relates to the following systems which underpin National Ambulance Critical activities:

Service	DR Method
1. Telephony (998) services	Fully Redundant
2. Internet connectivity	Fully Redundant
3. Critical Applications	15 min Recovery

With a key objective of providing fully redundant or recovery within 15 minutes of the IT DR plan being triggered.

The following NA policies, standards and regulations relate to this plan:

- NCEMA - AE/SCNS/NCEMA 7000:2015 Business Continuity Management Standard (Specifications).

5. Roles and Responsibilities

IT DR Team

Designation	Responsibility	Contact details
Business Continuity Plan Owner	– Ensure all DR and BCP plans are current and tested	TBC
NA Executives	– Approving DR trigger	TBC
NA Directors **ACC Manager**	– Act cooperatively with another member from this group to trigger the DR Plan. – Mobilizing DR Team once triggered. – Inform Executive of that DR Plan has been activated.	TBC
IT Manager **QHSE Manager** **ACC Manager**	– Mobilizing DR Team on receipt of a DR Trigger alert. – Coordinate resource and communication.	TBC
IT DR Implementation Team	– Implementing DR Plan and recovery.	TBC

6. Authority to Activate IT DR Plan

- Any National Ambulance Executive may invoke or trigger the DR plan as an individual.
- Two or more National Ambulance Directors plus the ACC Manager may invoke or trigger the DR plan should an executive not be available at the time of the incident leading to the trigger.

7. Criteria for Activating Plan

The IT DR plan should be triggered when any of the following criteria is met or is highly likely to occur in a reasonable time period, for example:

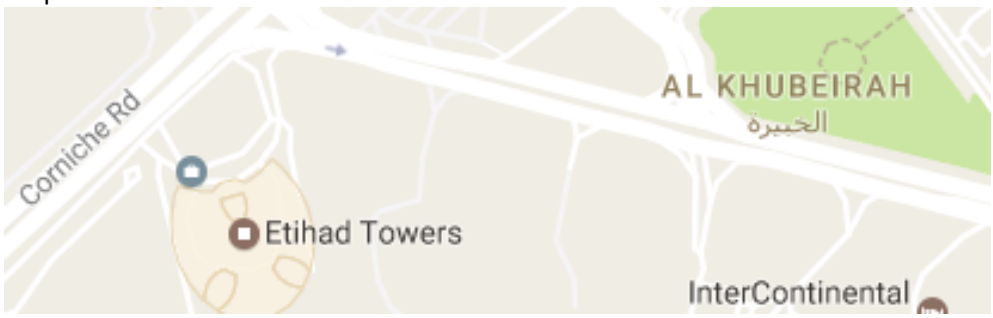
- Fire, Flood, or other environmental impact such as high winds or storms.
- Prolonged loss of power, cooling, telephony, network or access to the primary location (Head Office).
- Software, Hardware or other failure.
- Malicious activities such as hacking, computer virus or worm, denial of service attack, or other cyber attack

Which disables IT services or makes the provision of IT services from the primary location unstable or at a high risk of failure.

8. Primary and Backup locations

Primary Location
National Ambulance Head Office
Floors 6 and 7, Tower 3, Etihad Towers
Al Khubeirah Abu Dhabi

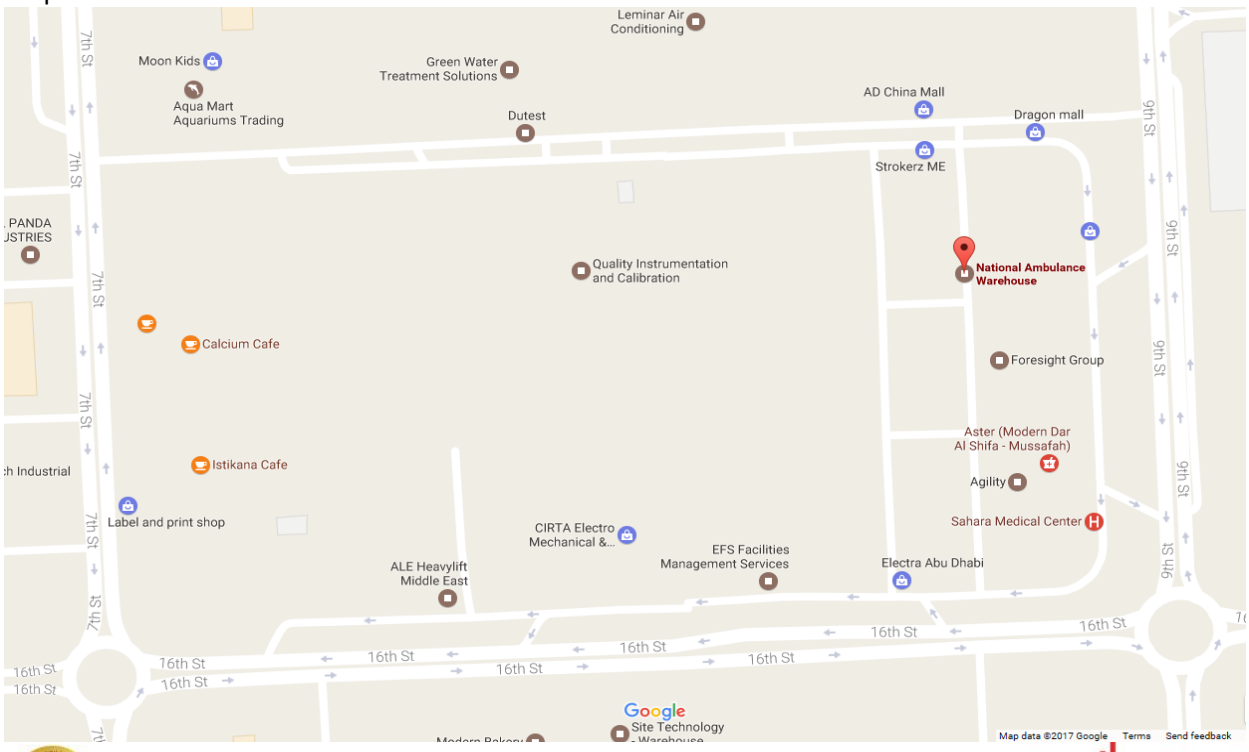
GPS Co-Ords: N24.45928, E054.32175
Map



Backup Location
National Ambulance Warehouse
Block M-45, 9th Street
Mussafah, Abu Dhabi

GPS Co-Ords: N24.34808, E054.4807

Map



9. Third Parties

	Name	Contact	Response Time	Services
Etisalat	Helpdesk	8009111		PRI Lines
	Santosh Ramkrishna (Account Manager)	971-502333729		MPLS Line
				Internet Lease Line
AGC	Muhammad Faiez	971-555464495		AVAYA IPT
	Helpdesk	customercare.mea@agcnetworks.com	4 hr	
		971-43649009		
DD	Ramy Haidar (Account Manager)	971-505367829		Exsi Server
	Helpdesk	support.mea@dimensiondata.com	4 hr	VMWARE
	Phone (24 X 7) - Within UAE	800 DDATA / 800 33282		EMC Storage
	Phone (8 X 5) - Outside	971- 4368 9902 (During Office Hours)		
	Phone (24 X 7) - Outside UAE	27 11 575 2523 (After Office Hours)		
Softec	Mayda	971-551571720		CAD
	May - Egypt number	20-120 0003119		BI
Sanco	Faizan	971-6555 1800		MDT Hardware
		faizan.mahboob@sanco-me.com		
Smart360tech	Mr. Paul Helpdesk	support@smart360tech.com	4 hr	CICSO IPT
	Phone 8x5	971-42943329		
	Mobile 24x7	971-5539 24081		
		971-5531 50615		

10. Impact of Disruption on Prioritized Activities over Predetermined Timeframes

All services will auto failover or be recovered within 15 minutes of the DR plan being triggered.

10.1. Resources required for recovery

Each member of the IT DR team requires:

- Phone / SMS
- IT DR Contacts list

In addition, each member of the IT DR Implementation Team requires:

- Backup Site Access or
- Backup Site Remote Access via VPN and Internet
- Backup System Admin Account and Password
- IT DR Recovery procedures and critical applications startup priority lists

10.2. DR Plan Activation Procedure

The authorized National Ambulance Directors, ACC Manager or Executive may invoke DR by calling one of the following staff members and instructing them to implement the IT DR Plan giving the nature of the incident which caused the DR plan trigger and any additional information as may be required to assist in execution:

- IT Manager
- QHSE Manager
- ACC Manager

These parties will then invoke the IT DR Plan and start mobilizing the IT DR Implementation team.

10.3. Prioritized objectives

The services will be prioritized in the following order:-

Service	DR Method
1. Telephony (998) services	Fully Redundant
2. Internet connectivity	Fully Redundant
3. Critical Applications	15 min Recovery

With the IT DR Implementation team tasked to test and verify the fully redundant services before starting to recover the critical applications.

10.4. Recovery and stand-down

Once the emergency has ended or the event which triggered the implementation of DR has been resolved the following steps will be taken by the IT Manger, QHSE Manager or ACC Manager with assistance from the IT DR Implementation team, in order to return to normal operations.

1. An Assessment of the Primary Site as to its suitability to resume IT Services
2. An Assessment of Hardware, Software and Data as to its state.
3. Draft a recovery plan to address any issues found in the above assessments
4. Inform the IT DR Team of any issues which would prevent recovery
5. Agree and implement the recovery plan

On completion of the recovery plan, the IT DR Team will meet and review the following areas with a view to improving processes and removing issues and root causes from the environment.

1. Review the cause of the incident to determine if it could have been avoided and assess the likelihood of reoccurrence
2. Review the DR Plan, assess what worked and what can be improved on.
3. Review the incident log and activities to implement DR, assess what worked and what can be improved on
4. Assess whether normal operations has been achieved and detail any outstanding issues to be resolved.

11. Testing

Testing will be carried out according to the Test Schedule below. A Test Plan will be developed for each test, based on a review of past service outages, incident logs and incident register affecting IT services and service criticality. Staff members and third-parties responsible for planning, conducting and reviewing test outcomes will be identified. Advance notification of the plan will be issued to operations that may be affected by testing, and commencement of testing will be authorised by the IT Manager.

Testing types may range in complexity, risk and resources required:

- Desktop review – plan owner review existing arrangements and documents;
- Desktop walkthrough – IT DR team review plan step by step, may involve third-parties;
- Scenario testing – a test scenario is developed and workshopped with IT DR team;
- Partial or full simulation
- Live testing – eg full physical drill and shutdown of services.

IT Service Test Schedule

Service/ Equipment	Test Type	Objective	Frequency / Quarter
Telephony (998) services	Partial simulation	Test Phone system and 998 redundancy	Quarterly
Internet connectivity	Partial Simulation	Test Internet redundancy	Q2
Critical Applications	Desktop Review	Ensure all procedures are up to date	Q2
	Partial simulation	Ensure DR processes are working	Q2
Data Backup	Partial simulation	Test Restore of Critical Data	Monthly

12. Document Configurations Control Date

A review and update of this document will take place as necessary, when changes occur that identify the need to revise this Policy such as changes in roles and responsibilities, release of new legislative or technical guidance, or identification of a new policy area.

This document ownership for editing is identified as:

Chief Administration Officer

Change Brief

Version No.	Date	Changes
1.0	April 2017	New document

Review & Approval: _____ Date:_____

_____
Wayne Wilkinson
Chief Administration Officer