Disaster recovery plan

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	8/30/2022		

Table of Contents

Information Technology Statement of Intent 3
Policy Statement.... 3
Objectives.... 3
Key Personnel Contact Info 5
Notification Calling Tree.... 5
External Contacts
External Contacts Calling Tree 7
Diagrame
Basic IT and Telecoms Diagram....9
Network diagram (visio)....10
1 Plan Overview.... 12
1.1 Updates.... 12
1.2 Documentation Storage.... 12
1.3 Backup Strategy.... 12
1.4 Risk Management 12
2 Emergency Response.... 15
2.1 Alert, Escalation and Plan Invocation 15
2.2 Disaster Recovery Team.... 15
2.3 Emergency Alert, Escalation and DRP Activation.... 15
3 Media.... 17
3.1 Media Contact.... 17
3.2 Media Strategies 17
3.3 Media Team 17
3.4 Rules for Dealing with Media.... 17
4 Financial and Legal Issues.... 18
4.1 Financial Assessment 18
4.2 Financial Requirements.... 18
4.3 Legal Actions 18
5 DRP Exercising.... 19
Appendix A – Technology Disaster Recovery Plan 21
Disaster Recovery Plan for <System One>.... 18
How to recover....25
Recovery disaster step by step....26
Appendix B – Suggested Forms 31
Damage Assessment Form 31
Management of DR Activities Form.... 31
Disaster Recovery Event Recording Form 31
Disaster Recovery Activity Report Form 32
Mobilizing the Disaster Recovery Team Form.... 32
Mobilizing the Business Recovery Team Form 33
Monitoring Business Recovery Task Progress Form.... 34
Preparing the Business Recovery Report Form 34
Communications Form.... 35
Returning Recovered Business Operations to Business Unit Leadership 35
Business Process/Function Recovery Completion Form.... 35

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure the physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, local/remote access to information systems and services, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to account for changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan that will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency that interrupts information systems and business operations. Additional objectives include ensuring the following:

- all employees must fully understand their duties in implementing the plan;
- operational policies are adhered to within all planned activities;
  • the proposed contingency arrangements are cost-effective,
  andmanagement must consider implications on other company
  sites.

1: Invoking disaster recovery

Disaster recovery plan

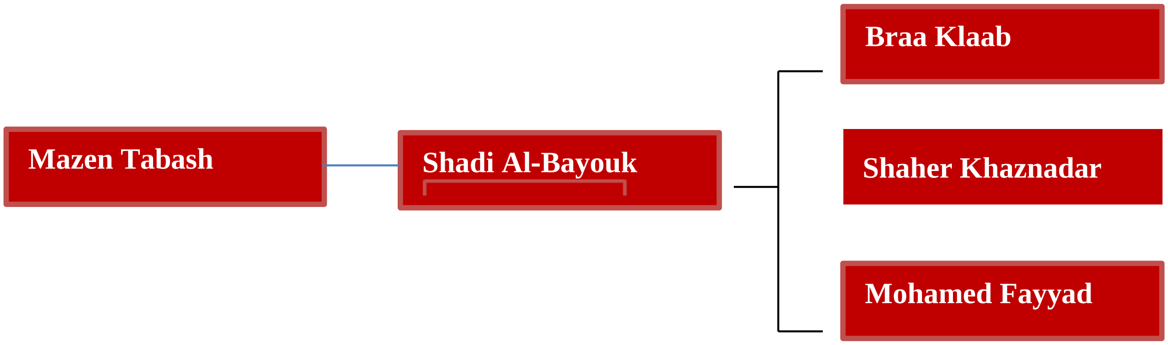
Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
Mazen Tabash	Work	Network department manager
	Mobile-in	112
	Mobile-out	0599864230
	Home	Abasan al-Kabira
Shadi Al-Bayouk	Work	Assistant director of network department
	Mobile-in	110
	Mobile-out	0592814315
	Home	Khan Yunis
Shaher Khaznadar	Work	Technical Support
	Mobile-in	222
	Mobile-out	0597329433
	Home	Khan Yunis
Mohamed Fayyad	Work	Technical Support
	Mobile-in	222
	Mobile-out	0595038181
	Home	Khan Yunis
Braa Klaab	Work	Technical Support
	Mobile-in	222
	Mobile-out	0598740079
	Home	Khan Yunis
	Work	
	Mobile-in	
	Mobile-out	
	Home	

External Contacts

Name, Title	Contact Option	Contact Number
Power Company		
	Work	Secondary power supply
	Mobile	133
Hardware Supplier (DEL provider)		
	Work	Technical Support
	Contact	https://www.dell.com/en-us/lp/contact-us
Hardware Supplier (HP provider)		
	Work	Technical Support
	Contact	https://support.hp.com/us-en/contact
Local Hospital		
	Work	Emergency Ambulance
	Mobile	2551244
Medical Supplies		
	Work	Emergency Ambulance
	Contact	101
Ministry of Telecom and Information Technology of the State of Palestine		
	Work	hosting
	Contact	166
Paltel		
	Work	internet provider
	Contact	199
fuion		
	Work	internet provider
	Contact	1700-100-800

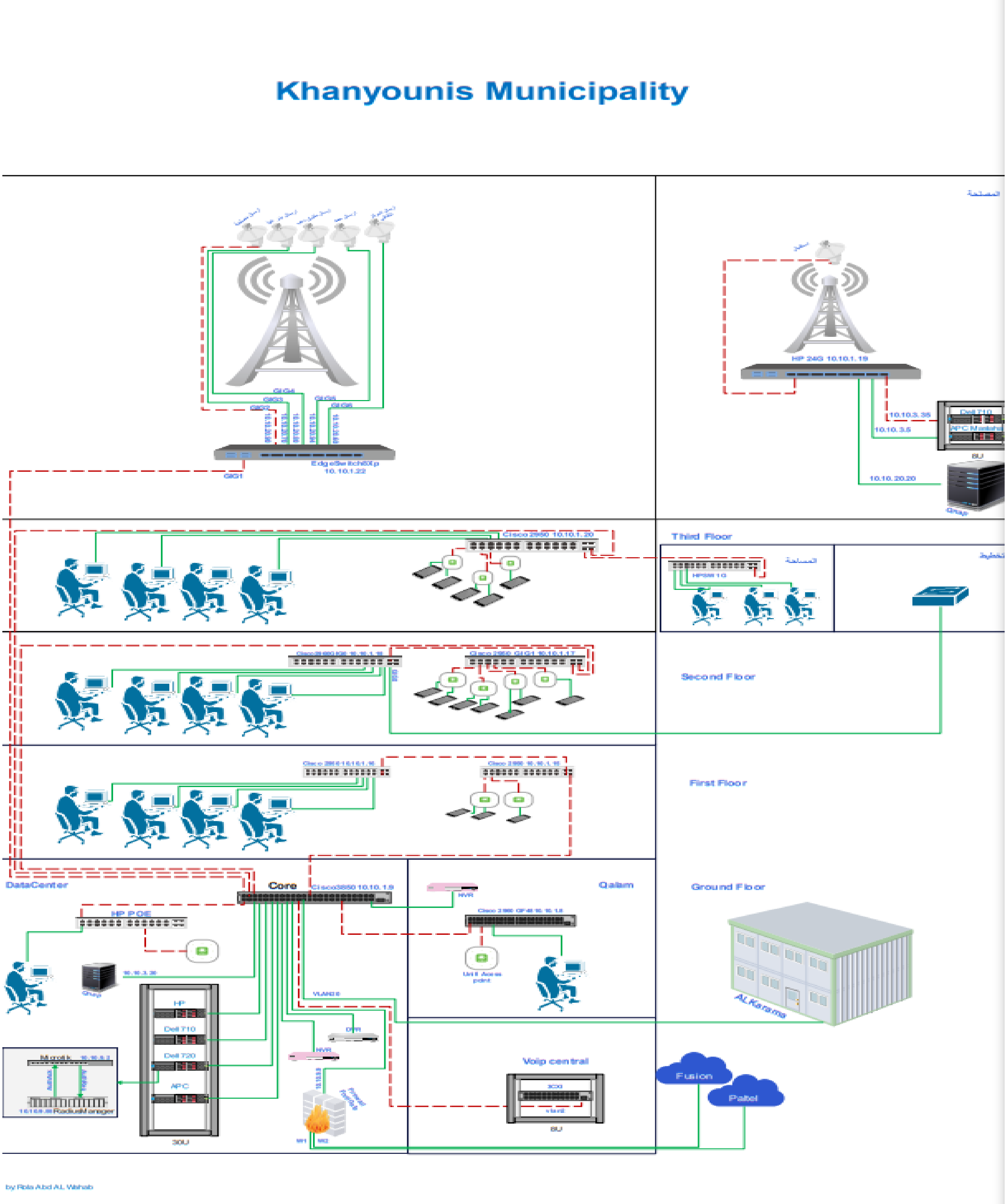
Contacts Calling Tree



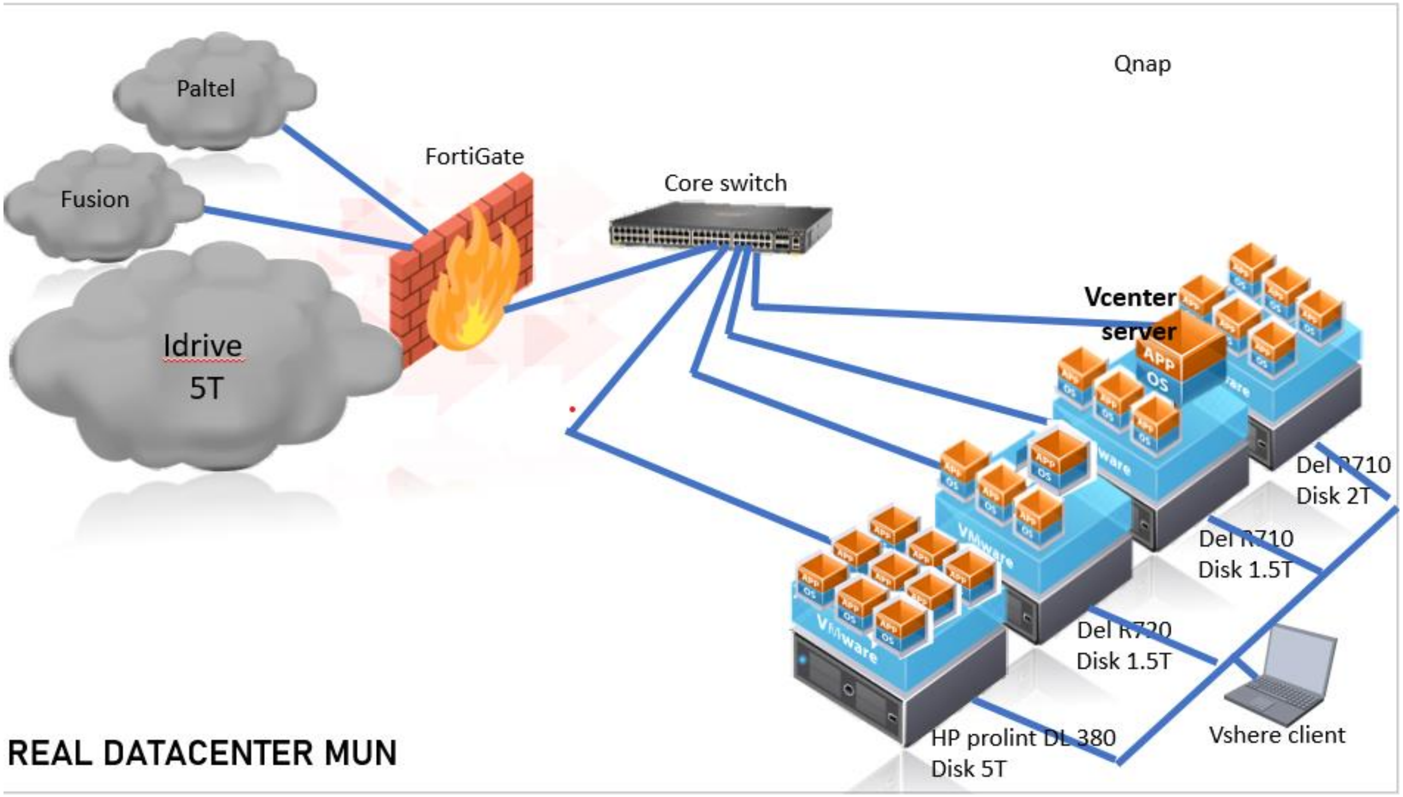
2: Diagrame

Disaster recovery plan

Basic IT and Telecoms Diagram



Network diagram (visio)



3: Disaster Recovery Plan

1 Plan Overview

1.1 Updates

It is necessary for the disaster recovery plan updating process to be properly structured and controlled. Whenever changes are made to the plan they must be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Director.

1.2 Documentation Storage

Digital and hard copies of this plan will be stored in secure locations to be defined by the company. Each member of senior management will be issued a digital and hard copy of this plan to be filed at home. Each member of the disaster recovery team and the business recovery team will be issued a digital and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

1.3 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is to copy the primary site to a secondary site on a schedule, Veeam program through wireless communications that connect the two sites on the level of virtual machines, And Acronis at the file level .It requires periodic maintenance of communications between the two sites and a careful examination to ensure the correctness of the backup copies.

1.4 Risk Management

There are many potential disruptive threats that can occur at any time and affect normal business processes. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster (Hardware)	Probability Rating	Impact Rating	How to cover it
Network Cable Failure	1	1	Multi NIC with Multi Cable and Enable Teaming
Network Card Failure	1	1	Multi NIC with Multi Cable and Enable Teaming
Power Cable Failure	2	4	Multi Power Cables or more connect with Multi Power Supply
.Power Supply Failure	1	1	Multi Power Cables or more connect with Multi Power Supply
Server H/W Failure	1	1	Build Server Cluster
Storage HDD Failure	2	2	Configure H/W RAID
Storage Node Failure	1	1	Storage Have 2 Storage Processors Nodes.
Air condition	1	3	Have Another Air Condition
UPS Failure	1	1	you con work by Generator
Generator Failure	2	5	it's last stage if lost all Public Power then UPS then Generator you must move to DR.
Public Power Failure	1	1	you can work by UPS and Generator

Potential Disaster (software)	Probability Rating	Impact Rating	How to cover it
Windows Or Linux OS Corruption	2	2	Snapshot, Repair OS, Restore from Backup.
Application Corruption	3	3	Restore Configurations, Reinstall App
Database Corruption (Oracle or SQL)	4	5	Restore from Backup by veeam backup
VMware Virtual Machine Corruption	2	حسب أهميتها	Restore from Backup by veeam backup
VMware vSphere ESXI Failure	1	2	Restore from Backup by veeam backup
VMware vCenter Failure	1	2	Restore from Backup by veeam backup
Backup Application Failure	1	3	Rebuild Backup App or Restore from Backup
Backup Data Failure	1	3	Work from 2nd Copy from Different media or from Tapes.

Potential Disaster (network)	Probability Rating	Impact Rating	How to cover it
User Switches Failure	1	1	Replace by Another Switch from local store.
Core Switches Failure	1	5	Have another Core SW or Replace it and Move to DR during Replace it.
Internet Connections Failure	2	2	Have Multi Internet connection from Multi ISP.
Branch Connection Failure فشل اتصال بالفرع	5	3	Work by another MPLS from Different ISP or use 4G Connection.
Core Firewall Failure	2	4	Have Another Core FW or Move DR till Replace it.
Fully Datacenter Network Failure	1	5	Stop all opration

Probability: 1=Very High, 5=Very Low

Impact: 1=Total destruction, 5=Minor annoyance

2 Emergency Response

2.1 Alert, Escalation and Plan Invocation

2.1.1 Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DR plan are:

- Total loss of all communications
- Flooding of the premises
- Loss of the building
- Need to evacuate the building

2.1.2 Assembly Points

Where the premises need to be evacuated, the invocation plan identifies two evacuation assembly points:

- Primary – مبنى البلدية الرئيسي (غرفة مدير تكنولوجيا المعلومات)
- Alternate _ مبنى مصلحة المياه

2.1.3 Activation of Emergency Response Team

When an incident occurs the emergency response team (ERT) must be activated. The ERT will then decide the extent to which the DR plan must be invoked. All employees must be issued a quick reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- respond immediately to a potential disaster and call emergency services;
- assess the extent of the disaster and its impact on the business and data center;
- determine if an evacuation is needed;
- decide which elements of the DR plan should be activated;
- establish and manage disaster recovery team to maintain vital services and return to normal operations, and
- ensure employees are notified and allocate responsibilities and activities as required.

2.2 Disaster Recovery Team

The disaster recovery team will be contacted and assembled by the ERT. This team's responsibilities are to:

- establish facilities for an emergency level of service within two business hours;
- activate access to IT services for remote working within day;
- restore key services within baladia as soon as possible of the incident;
- recover to business as usual within 8-24 hours after the incident;
- coordinate activities with disaster recovery team and first responders, and
- report to the emergency response team.

2.3 Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that, in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

2.3.1 Emergency Alert

When using emergency alert systems, the person discovering the incident will call a member of the Emergency Response Team in the order listed:

Emergency Response Team

- Mohamed Fayyad
- Shaher Khaznadar
- Braa Klaab

If not available try:

- Shadi Al-Bayouk
- Mazen Tabash

The emergency response team is responsible for activating the DR plan for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the disaster recovery team that an emergency has occurred. The notification will request disaster recovery team members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The business recovery team will consist of senior representatives from the main business departments. The business recovery team leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

2.3.2 DR Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed. Management should be prepared to order employees to work remotely.

2.3.3 Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster. Employees should be prepared to work remotely if assigned.

2.3.4 Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

2.3.5 Recorded Messages / Updates

For the latest information on the disaster and the organization's response, staff members can call a toll-free hotline provided to each employee. This may be provided to them through email, text message or a hard copy wallet card. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

2.3.6 Personnel and Family Notification

If the incident has resulted in a situation that would cause concern to an employee's immediate family, such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly. If employees are ordered to go home and work remotely, they should notify family members of that change as soon as possible.

3 Media

3.1 Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with communications during and after the event.

3.2 Media Strategies

1. Avoid adverse publicity
2. Take advantage of opportunities for useful publicity
3. Have answers to the following basic questions:
    - What happened?
    - How did it happen?
    - What are you going to do about it?

3.3 Media Team

- _Mohamed Fayyad
- Shaher Khaznadar
- Braa Klaab

3.4 Rules for Dealing with Media

Only the media team is permitted direct contact with electronic and print media; anyone else contacted should refer callers or in-person media representatives to the media team. Plans for social media use should be developed and distributed to all employees.

4 Financial and Legal Issues

4.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the effect of the incident on the financial affairs of the company. The assessment should cover:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

4.2 Legal Actions

The company legal department and emergency response team will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event, such as the possibility of claims by or against the company for regulatory violations.

5 DRP Exercising

Disaster recovery plan exercises, especially if remote working by employees is indicated, are an essential part of the plan development process. Plan exercises ensure that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities, and that the technologies are available and operational.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

4: Information System

Appendix A – Technology Disaster Recovery Plan For system

OVERVIEW	
PRODUCTION SERVER(32)	Location: MUN Server Model: HPE ProLiant MicroServer Gen10 Operating System: esxi 6 CPUs: xeon (4110) Memory: 64 G Total Disk: 5 T IP Address: 10.10.3.32 NIC: 4

BACKUP STRATEGY FOR SERVER s1		
VM	Full backup	Incremental backup
Fileserver (archive)	First Friday of every month	Saturday, Tuesday, Thursday 10 pm
Fileserver (employee)	First Monday of every month	Saturday, Monday, Wednesday 8 pm
Fileserver (project)	First Friday of every month	Sunday, Tuesday, Thursday 10 pm
ArcGis	every saturday	every day
oracle	Saturday Monday Wednesday	Every day 3 pm

OVERVIEW	
PRODUCTION SERVER(33)	Location: MUN Server Model: DEL R710 Operating System: esxi 6 CPUs: xeon (E5645) Memory: 80 G Total Disk: 1.5 T IP Address: 10.10.3.33 NIC: 4

BACKUP STRATEGY FOR SERVER 33		
vm	Full backup	Incremental backup
Web server	First Friday of every month	Saturday, Tuesday, Thursday 10 pm
Windows deployment	First Monday of every month	Saturday, Monday, Wednesday8 pm
API	First Friday of every month	Sunday, Tuesday, Thursday 10 pm
developer	every Saturday	every day
S3	Saturday Monday Wednesday	Every day 3 pm
3CX VOIP	Monday every week	Monday, Thursday 3 pm
PRTG	First Thursday of every month	Scand Sunday of every month
OMSA	First Thursday of every month	

OVERVIEW	
PRODUCTION SERVER(34)	Location: MUN Server Model: DEL R720 Operating System: esxi 6 CPUs: xeon (4110) Memory: 64 G Total Disk: 2.5 T IP Address: 10.10.3.34 NIC: 4

BACKUP STRATEGY FOR SERVER 34		
VM	Full backup	Incremental backup
VCenter	Monday, Thursday 5 pm	Every Saturday
manager	First Monday of every month	Saturday, Monday, Wednesday
S4	Every Saturday	Every Friday 2

OVERVIEW	
PRODUCTION SERVER(35**)**	Location: MUN Server Model: HP prolint DL300 Operating System: esxi 6 CPUs: xeon (4110) Memory: 50 G Total Disk: 2 T IP Address: 10.10.3.35 NIC: 4

BACKUP STRATEGY FOR SERVER 34		
VM	Full backup	Incremental backup
Quety sw	First Monday of every month	Every friday of every week

How to Recover

RECOVERY

Use this table to outline the order in which you need to recover individual servers, according to the business priority.

Priority Order	Server Name	IP Address	Description
1	33	10.10.3.33	Domain Controller
2	32	10.10.3.32	database server
3	33	10.10.3.33	Application server
4	32	10.10.3.32	fileserver
5	34	10.10.3.34	vcenter

Recovery disaster step by step

Use these templates to create your own recovery plans in accordance with your own recovery processes.

Recovery1: Operating system software corrupted

	Possible Actions	Who is responsible?
Step 1	Windows Recovery	IT Admin
Step 2	RESTOR vm	IT Admin
Step 3	Windows Live CD or Flash	IT Admin
Step 4	Boot from the CD	IT Admin
Step 5	Retrieve files from disks C,D	IT Admin

Recovery2: Application failed

	Possible Actions	Who is responsible?
Step 1	Generate new app	IT Admin
Step 2	Install it on the server	IT Admin

Recovery3: esxi corrupted

	Possible Actions	Who is responsible?
Step 1	Go to the vmware website	IT Admin
Step 2	VMware Compatibility list	IT Admin
Step 3	Enter server specification	IT Admin
Step 4	Burn the program to media	IT Admin
Step 5	boot server from media	IT Admin
Step 6	Update to the new version	IT Admin
Step 7	Reboot the server	IT Admin

Recovery4: database corruption

solution 1

	Possible Actions	Who is responsible?
Step 1	Attempt to fix the problem	IT Admin
Step 2	Check the logs to determine the cause of the failure	IT Admin
Step 3	Fix the error based on the error number	IT Admin

solution 2

	Possible Actions	Who is responsible?
Step 1	Determine the last working point of the veeam	IT Admin
Step 2	Make a restoring	IT Admin

Solution 3 (if system backup fiald)

	Possible Actions	Who is responsible?
Step 1	Create a new vm	IT Admin
Step 2	Create a new database oracle system	IT Admin
Step 3	Restor data from dump file	IT Admin
Step 4	Try to collect lost data through the help of staff	IT Admin

Recovery5: Server H/W Failure

Solution1

	Possible Actions	Who is responsible?
Step 1	Prepare a new server	IT Admin
Step 2	stats how many vm failed	IT Admin
Step 3	Restore the latest version of veeam	IT Admin

Solution 2

	Possible Actions	Who is responsible?
Step 1	Trying to fix the malfunction	IT Admin
Step 2	Attempt to recover disk data through another server	IT Admin
Step 3	Restore raid configuration settings and insert them into the new server	IT Admin
Step 4	Mounting data store	IT Admin
Step 5	data recovery	IT Admin
Step 6	run vm	IT Admin

Recovery6:firewall failed

	Possible Actions	Who is responsible?
Step 1	Do a factory reset	IT Admin
Step 2	Buy Firewall Software and deal with it	IT Admin

Recovery7: Internet Connections Failure

	Possible Actions	Who is responsible?
Step 1	Run the backup line	IT Admin
Step 2	Check with your service provider to determine the problem	IT Admin

Recovery8: Branch Connection Failure

	Possible Actions	Who is responsible?
Step 1	Check the communication tunnel or component	IT Admin
Step 2	Check other connection channel and adjust settings or Replace damaged components	IT Admin

Recovery9: Full Datacenter Network Failure

	Possible Actions	Who is responsible?
Step 1	Network Diagnostics	IT Admin
Step 2	Disconnect all network components except server 1 and pc 1	IT Admin
Step3	Add one server after another	IT Admin

6: Documenting the disaster

Appendix B – Suggested Forms

Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

Management of DR Activities Form

During the disaster recovery process all activities will be determined using a standard structure. Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period. All actions that occur during this phase will need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

Disaster Recovery Event Recording Form

All key events that occur during the disaster recovery phase must be recorded. An event log shall be maintained by the disaster recovery team leader. This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.

The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

Description of Disaster:
Commencement Date:
Date/Time DR Team Mobilized:

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

Disaster Recovery Team's Work Completed: <Date>
Event Log Passed to Business Recovery Team: <Date>

Disaster Recovery Activity Report Form

On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken. The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions. The report will also contain an assessment of the impact to normal business operations.

The report should be given to business recovery team leader, with a copy to senior management, as appropriate. A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response. In addition to the business recovery team leader, the report will be distributed to senior management

The report will include the following:

- A description of the emergency or incident
- People notified of the emergency
- Dates people were notified
- Action taken by members of the disaster recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the business continuity plan and lessons learned
- Lessons learned

Mobilizing the Disaster Recovery Team Form

Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.

The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed.

Description of Emergency:
Date Occurred:
Date Work of Disaster Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments/Specific Instructions Issued					

Mobilizing the Business Recovery Team Form

Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.

The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

Description of Emergency:
Date Occurred:
Date Work of Business Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments/Specific Instructions Issued					

Monitoring Business Recovery Task Progress Form

The progress of technology and business recovery tasks must be closely monitored during this period of time. Since difficulties experienced by one group could significantly affect other dependent, tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated.

Note: A priority sequence must be identified, although, where possible, activities will be carried out simultaneously.

Recovery Tasks (Order of Priority)	Person(s) Responsible	Completion Date		Milestones Identified	Other Relevant Information
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Preparing the Business Recovery Report Form

On completion of business recovery activities, the business recovery team leader should prepare a report on the activities undertaken and completed. The report should contain information on the disruptive event, who was notified and when, action taken by members of the business recovery team, together with outcomes arising from those actions.

The report will also contain an assessment of the impact to normal business operations. The report should be distributed to senior management, as appropriate.

The contents of the report shall include the following:

- A description of the incident
- People notified of the emergency
- Dates people were notified
- Action taken by the business recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Problems identified
- Suggestions for enhancing the disaster recovery and/or business continuity plan
- Lessons learned

Communications Form

It is critical during the disaster recovery and business recovery activities that all affected persons and organizations are kept properly informed. The information given to all parties must be accurate and timely. In particular, any estimate of the timing to return to normal working operations should be announced with care. It is also important that only authorized personnel deal with media queries.

Groups of Persons or Organizations Affected by Disruption	Persons Selected To Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Stakeholders			
Others			

Returning Recovered Business Operations to Business Unit Leadership

Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader. This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to business-as-usual.

It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead. It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team.

Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management (If different than completion date)	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name:
____

Signature:
____

Date: __________________________

(Any relevant comments by the business recovery team leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions.

Name:
____

Title:
____

Signature:
____

Date: __________________________