a) Incident declaration, escalation, notification, mobilisation and response,
b) response preparation and planning,
c) communications with the DMAT and other stakeholders,
d) media management,
e) safety of all personnel and visitors,
f) Incident close-off and debriefing and revision of plans as needed,
g) Training and exercise,
h) On-going review.

Notwithstanding the above, the following are some possible emergency situations in the system, and the adopted systematic approach incorporates reliability and communication features to minimize the occurrence of emergency situations where possible, and to enhance safety, response, and communication when emergencies occur.

11.16.2 Pump Station Failures

The ERP should include in addition to the procedures on the following items:

a) Emergency Contact List: The list designates someone from Consultant / Contractor / DMAT to be contacted in case of emergency regardless of the day of the week or time of day. The list shall be kept up-to-date and make available to wastewater system personnel.
b) Keys of all facilities main gate, building doors, MCC room, generator room, dry well/wet well/chamber access, etc. All keys shall be kept and tagged at known location.
c) Emergency teams with tools/equipment/spare parts/transportation shall be assigned and available 24 hours a day and during holidays/week ends.
d) Phones list of all utilities including: electricity, water, police, civil defence, Etisalat, agricultural DMAT, and hospital.
e) Weekly report for Emergency Generators status and diesel fuel inventory stocked levels.
f) List of first point of flooding at each pump station in case of switched off the pump station.
g) Maps and as-built drawing for the sewage system to be stored in a secure location. Policy for the release of copies of maps, records, drawings and other sensitive information.
h) Plan to test ERP / Contact list at least annually.
i) Information technology: Computer access password to be protected, virus protection to be installed and up-to-dated. SCADA system to be operated on systems without Internet access to reduce the chance of unauthorized access, SCADA system to be evaluated for weaknesses of potential intruders (penetration testing). Plan to back up computer data / PLC, backing up data regularly will help prevent the loss of data in the event of power outages or damage to the computer, backup copies of data to be kept at a secure off-site location, use of surge protectors can help to reduce damage to computers.
j) Physical Assets: Perimeter and Access Control: restrict access to the critical components of wastewater system to authorized people only, Post sign restricting entry to authorized personnel only. All facilities should have a security fence around the perimeter, all gates, doors and windows to be closed/locked. System should ensure that all security measures comply with safety regulations and fire codes. Adequate external lighting to be around facilities, Warning signs (against