

# SITE BUSINESS CONTINUITY PLAN

## FOR THE PROVISION OF DATACENTER SERVICES FOR DNAS & DRAS

Copy No:

---

### **FUTURE READY IT-HOUSING**

---

#### **CONTROLLED DOCUMENT**

No photocopying of this document is permitted. Copies of this document should only be obtained from DigiPlex. Any amendment requirements, or suggestions, should be forwarded to the Site Manager.

---

#### **COMPANY CONFIDENTIAL**

This document is for the sole use of DigiPlex. It may not be reproduced in any form, part or whole, without the prior written approval of the Site Manager, DigiPlex.

This document will only be issued to other parties on their agreement that it shall not be used in any form, except for that purpose for which it is intended and agreed.

---

Document Number:  
BCP-MAN-01-00-DNAS &  
DRAS

Revision:  
A

Issue Date:  
September 2018

Owner  
Site Manager



## Contents

Plan Distribution and Access .....	3
Plan Distribution List .....	4
Business Continuity Plan Review and Amendment.....	4
Record of Review.....	4
<b>1.0 Introduction .....</b>	<b>5</b>
1.1 Purpose.....	5
1.2 Scope and Objectives .....	6
1.3 Definitions .....	6
1.4 Roles and Responsibilities.....	6
1.5 Process Overview .....	7
1.6 Risk Assessment .....	8
1.7 Crisis Prevention.....	9
1.8 Records.....	9
1.9 Ending the Crisis.....	9
1.10 Learning the Lessons .....	10
1.11 Crisis Training.....	10
1.11.1 General.....	10
1.11.2 Training.....	11
1.11.3 Exercises .....	11
<b>2.0 Escalation Levels .....</b>	<b>14</b>
<b>3.0 Emergency Contact Information .....</b>	<b>16</b>
3.1 Crisis Management Team.....	16
3.2 Emergency Response Team .....	16
3.3 Key Suppliers Emergency Contact Information.....	17
<b>4.0 Emergency Response Procedures .....</b>	<b>18</b>
4.1 Fire.....	18
4.2 Bomb or Terrorist Threat .....	19
4.3 Civil Disturbance .....	21
4.4 Power Outage .....	22
4.5 Water Incident.....	23
4.6 Severe Weather .....	24
4.7 Snow Storm .....	Feil! Bokmerke er ikke definert.
4.8 Hazardous Material Spill.....	25
4.9 Cooling Failure.....	27
<b>5.0 Appendices.....</b>	<b>27</b>

## Plan Distribution and Access

- The Plan will be distributed to members of the emergency response team and department heads. A master copy of the document should be maintained by the Site Manager The plan will be available for review by all employees.
- Provide print copies of this plan within the room designated as the Emergency Operations Control Centre (EOCC). Multiple copies should be stored within the Facility EOCC to ensure that team members can quickly review roles, responsibilities, tasks, and reference information when the team is activated.

- Electronic copies should also be stored on a secured USB flash drive for printing on demand.

## Plan Distribution List

Copy No	Position	Name
1		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

## Business Continuity Plan Review and Amendment

- The Content of this plan shall be reviewed annually or will change in response to new business and client needs and new technology or resource related changes occur.
- The Site Manager shall be responsible for the control of all changes to this Plan. Any amendment requirements or suggestions shall be forwarded to the Site Manager for consideration and necessary action.
- The Site Manager may up-issue and distribute this plan in its entirety following annual review or where significant changes are required.

## Record of Review

Date Review Carried Out.	Reason for Review	Name of Reviewer	Amendment Action Required Yes/No

## 1.0 Introduction

Dealing with a crisis is the most demanding challenge likely to face DigiPlex. The crisis may result from a fire or other catastrophic incident affecting the company's business continuity, a major accident or some form of business crisis. The ability to manage the crisis effectively, to handle the media issues and to restore normal operation will determine whether DigiPlex survives the experience.

**Business continuity** encompasses planning and preparation to ensure that DigiPlex can continue to operate in case of serious incidents or disasters and can recover to an operational state within a reasonably short period. DigiPlex's business continuity includes three key elements and they are:

1. **Resilience:** critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions, for example using redundancy and spare capacity;
2. **Recovery:** arrangements should be made to recover or restore critical and less critical business functions that fail for some reason.
3. **Contingency:** DigiPlex has established a generalised capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

## 1.1 Purpose

This document provides a structured approach to the emergency management activities to ensure that DigiPlex will respond effectively to a crisis in whatever form it might take, establishes initial procedures and defines key responsibilities for the appropriate response to business disruptions that might threaten personnel, buildings, daily operations, DigiPlex's and customer reputation.

The principles behind this plan are:

- Risks are assessed for both probability and business impact
- Emergency Response Plans must be reasonable, practical and achievable

In other words, we are not planning for every possibility. Diminishing returns affect the benefits of planning for extreme cases.

Other functions of the Site Business Continuity Plan are as follows:

- Describe preventive measures that decrease the risk of a crisis event.
- Promote personal accountability and responsibility and the safe evacuation/invacuation of individuals.
- Lessen the possible impact on our operations.
- Establish procedures that can help us quickly and correctly deal with an emergency or crisis situation.

- Establish a process of regularly training and testing of our emergency response plans.
- Learning Lessons from every practice.

This Plan should be read in conjunction with the Crisis Communications Manual, CCOM-MAN-01-01-DGS, which provides advice and recommendations on how to manage communications in a crisis.

## 1.2 Scope and Objectives

This plan is applicable to all employees, visitors, and critical suppliers of DigiPlex at our DNAS and DRAS facility.

The measures described are designed to promote business continuity for Technical Infrastructure, Operations personnel, reduce response times, and enhance mitigation of a crisis.

The primary objective of this Site Business Continuity Plan is to

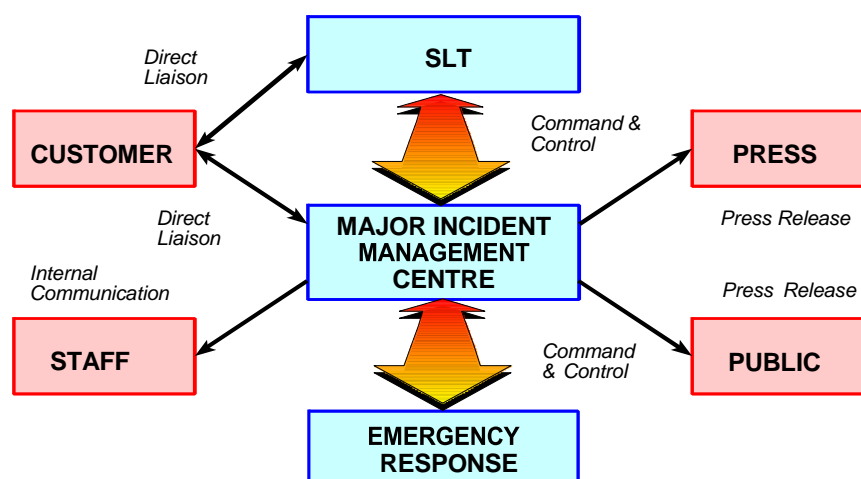
- Be prepared to respond to significant emergency scenarios, recover from them, and mitigate impact to our operations.
- Restore operations quickly and effectively.
- Help coordinate information internally and externally to our customers.
- Facilitate information dissemination and crisis communications to our stakeholders internally and customers externally.

## 1.3 Definitions

- EOCC- Emergency Operations Control Centre
- ERT- Emergency Response Team

## 1.4 Roles and Responsibilities

The diagram below shows the Roles and functional elements



The roles and responsibilities of the functional elements are:

- Senior Leadership Team (SLT) - Responsible for the overall direction of the crisis management response and for making timely executive decisions as required. The Senior Leadership Team will retain responsibility for the on-going management of the business not affected by the crisis.
- Crisis Leader (CEO/COO) - Responsible for the management of the Crisis Management Team and supporting staff and will have delegated executive authority to take the necessary measures to bring the crisis under control. The Crisis Leader is responsible for briefing the SLT and implementing their decisions.
- Emergency Response Team - Responsible for the execution, monitoring progress and reporting achievement, of agreed actions. The Emergency Response Team leader is the Head of Operations and is responsible for briefing the Crisis Management Team and implementing their decisions.
- Human Resources Team. Responsible for the HR aspects of the crisis including notification of family/relatives of staff affected by the incident, handling the immediate and long-term needs of the families and supporting other staff affected by the incident.
- Technical Advisors - Responsible for providing specialist technical advice as required covering areas such as technical, legal, political and financial issues.
- Liaison Staff. There may be a need to appoint staff responsible for liaison with emergency services, regulatory authorities or other parties directly involved. It may also be necessary to send senior staff to the scene of the incident to act as a spokesman for the company.

## 1.5 Process Overview

Part of good management practice is the preparation of plans covering predictable events. Although a crisis is unlikely to be predictable, many crisis situations can be identified and appropriate crisis planning measures can and should be taken against these scenarios.

Managing a crisis effectively (or preventing an incident becoming a crisis) will depend on speed of response and this means having in place:

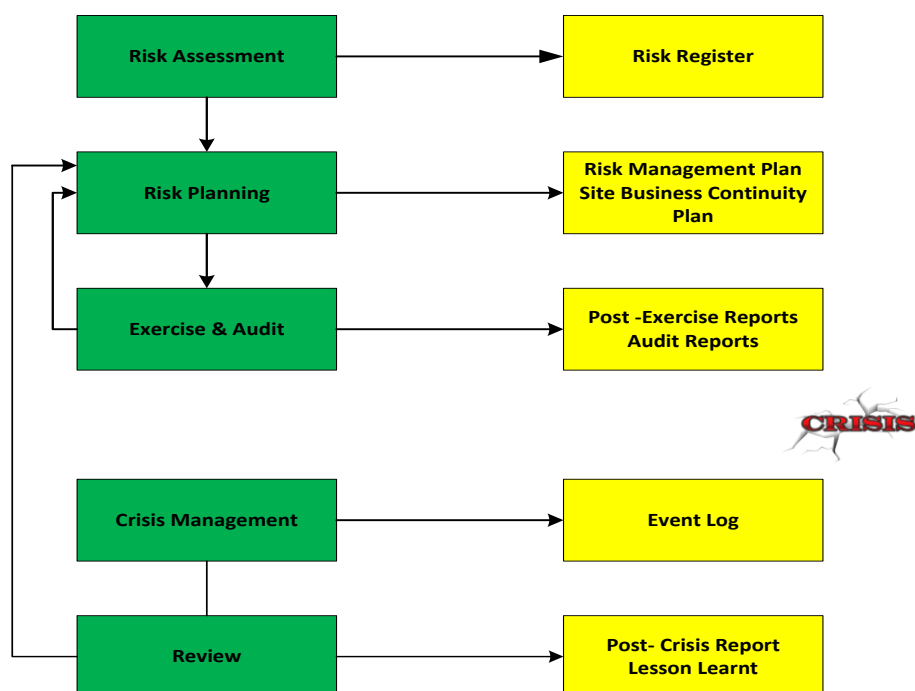
- Clear procedures and lines of responsibility
- Staff and other resources that can be activated at short notice to deal with a crisis
- Agreed principles for dealing with the media
- Instant access to relevant background information which will be required by media and others

The key stages in preparing for a crisis are:

- Risk Identification and Assessment
- Risk Planning
- Training
- Review/audit

The aim of these activities will be to reduce the likelihood of a crisis as far as practicable and to prepare contingency plans for critical risks.

The figure illustrates these key activities and identifies the main outputs. The existence of an appropriate Crisis Management Plan that can provide a framework for the crisis management actions is a vital part of the whole management process.



## 1.6 Risk Assessment

The first stage in any crisis management process is to carry out a detailed risk assessment. This will normally be undertaken as part of the normal project or business risk assessment process and will identify a number of risks whose potential impact on the business is sufficiently severe for more detailed risk assessment activities to be undertaken.

The "Risk Management Process", MAN-03-00-DGS describes the process of risk assessment. Identify possible threats to the business that could have a catastrophic impact on DigiPlex's business. Consider how these risks can be reduced and implement the necessary changes.

Identify situations (and combinations of situations) which could develop, and which could constitute a crisis. Identify those who may be affected (both within the organisation and externally) and how communication about a crisis would be handled. Although the aim will be to anticipate all possible crisis situations, it is still essential to prepare for the unexpected.



## 1.7 Crisis Prevention

To avoid the circumstances which can lead to a crisis situation, it is essential that policies and practices are put in place which identify and control risks. These systems and the training given to the individuals operating them are likely to be very closely scrutinised during a crisis and in any subsequent inquiry. Key systems include:

- **Internal control processes (ISO 9001)** designed to ensure compliance with corporate governance requirements and protect the value and assets of DigiPlex.
- **Safety management systems (OSHAS 18001)** designed to ensure compliance with all statutory Health and Safety legislation, prevent accidents and provide a safe and healthy working environment.
- **Environmental protection systems (ISO 14001)** designed to meet all statutory environmental protection requirements and to reduce any adverse impact on the environment.
- **Special management systems (ISO 27001)** relating to activities such as Information Security.

## 1.8 Records

A formal record of events is an essential document both for the immediate management of the crisis and for the subsequent analysis of the crisis to learn any lessons. It is possible that such a log may have to become evidence in any legal proceedings arising from the crisis. The log is used to record information received, the decisions made and by whom and any communication with external bodies. The information recorded will provide a verifiable chronology of events from the start. For each incoming and outgoing message and any significant event or decision, the following information must be recorded:

- a. Date and time of message/event/decision
- b. Message originator – name, organisation, contact number
- c. Message recipient
- d. Summary of information
- e. Action taken
- f. Initials to confirm that the necessary action has been taken

A possible format for a log is shown below in section 5 appendices.

## 1.9 Ending the Crisis

The management of the crisis should not stop until the crisis is truly resolved. Removing the crisis management measures is an important decision that should be made by the Crisis Manager after an in-depth examination. The following issues should be addressed:

- Declare an end to the crisis - It is most important for the company to signal an end to the crisis situation

- Follow up - Stay in touch with the community after a crisis, especially with those directly affected. Keep the media informed of any updates in the situation, and let them know the crisis has ended
- Make amends to those affected and then do whatever is necessary to restore your company's reputation in the community
- Assist staff in coming to terms with their experience. Staff who exhibit signs of trauma following a crisis or request assistance in coming to terms with their experience should be referred for professional debriefing and counselling as necessary
- Have a formal debriefing - Debrief members of your crisis management team. Analyse the outcome and the media coverage - both positive and negative
- Persons and organisations that have helped in the crisis should be thanked in writing
- Change internal policies or institute new ones to minimise a repeat of the crisis
- Revise this Business Continuity Management plan to reflect what has been learned

## 1.10 Learning the Lessons

An investigation should be carried out in accordance with the Control of Incident and Non-conformances procedure QA-PROC-06-00-DGS, as soon as the crisis is declared over, to determine what went wrong and how the problem was handled. A well-planned debriefing will address the psychological aspects of the crisis and provide information to help improve the crisis management plan. Each participant in the crisis management team and the main contributors at the location of the emergency should complete a report of his actions, thoughts and suggestions for improvement.

The Crisis Manager should conduct a debrief of all those involved in the crisis. The results of the debriefing sessions should be used to improve the crisis plan and to identify changes in procedures or processes that are required.

## 1.11 Crisis Training

### 1.11.1 General

Training of key personnel is essential. Training will be required in several specialist areas such as handling the media and specific technical skills that might be required at certain sites as well as training and familiarisation of the whole Emergency Response Team in operating in a typical crisis environment. This training should precede any formal exercises to test specific aspects of a Crisis Management Plan.

Prior to any training taking place, the following steps need to have been taken:

- Potential crisis scenarios have been identified
- Key staff likely to be involved in the management of a crisis have been identified
- A training needs analysis has been performed

### 1.11.2 Training

Unlike the emergency services, responding to a crisis situation is not likely to be considered to be part of the normal day-to-day activities for the nominated crisis management team. The importance of training in a properly structured manner is important if the full potential of all the parties involved is to be realised. Key training topics that are likely to be relevant to those involved in a crisis response are:

- **Awareness.** All members of the Emergency Response Team should be aware of possible crisis scenarios and the crisis management organisation and procedures. Training should provide an overview of the key management issues, the importance of team-working and the effects of stress.
- **Crisis Management.** This should cover the issues associated with information collection and processing, decision-making under pressure and the team management. The effect of stress on individuals and teams should also be covered.
- **Media Relations.** Training should cover press and broadcast media communication, the preparation of media press statements and briefs and familiarisation with media handling techniques. For senior staff, likely to be involved in facing journalists, individual practical training in interview and news conference techniques should be undertaken.

### 1.11.3 Exercises

#### 1.11.3.1 General

Exercises are an important management tool for informing and motivating personnel and giving confidence to those who may be required to respond in a crisis. They bring together those who may be involved with responding to an incident and they allow scrutiny of their responses under controlled conditions. They also provide the only comprehensive way of realistically evaluating contingency plans.

Exercises should reflect reality as far as is practicable. They can establish and reinforce relationships between those taking part, often under stressful conditions. They bring people from different areas together to work as a team, to realise clear goals and to get to know and respect each other's strengths and weaknesses.

#### 1.11.3.2 Exercise Types

Exercises take four basic forms and their use is dependent on the state of development of the crisis management strategy and the target audience:

- **Seminar.** Seminar exercises are designed to inform participants about DigiPlex the procedures that would be used to respond to an incident. Those involved can be either new to the job, established personnel or those recently identified as key staff. This type of event will bring staff together to inform them of current developments and thinking. These events may take the form of lectures or panel discussions and are primarily designed to focus on one aspect of the response.

The emphasis of this type of exercise is on problem identification and solution finding rather than decision making.

- **Table-Top.** Table top exercises are small scale, pre-planned, paper based exercises which aim to test plans, procedures and people in a controlled environment. They provide the few players involved with an opportunity to interact with and understand the roles and responsibilities of the other stakeholders taking part. They can engage players imaginatively and generate high levels of realism. Participants will get to know the people with whom they may be working in responding to a crisis. Those who have worked together and know each other will provide a much more effective response than those who come together for the first time when a real crisis occurs.
- **Drills.** Drills consist of limited activation and mobilisation of personnel and response teams in response to a hypothetical crisis scenario. Drills offer opportunities for personnel to receive "hand-on" crisis management training, demonstrate their capabilities, and validate, to a limited extent, capabilities documented in crisis management plans. Drills can be distinguished from exercises by their limited depth and breadth of participation (generally 2-3 groups), focus on a subset of specific crisis/emergency objectives, involvement of only one or two sites or locations, and limited or no deployment of personnel or equipment. Realism plays an essential part in ensuring that key staff react to a crisis situation in the appropriate manner.
- **Live.** Live exercises range from a small-scale test of one component of the response through to a full-scale test of the whole organisation. Live exercises provide the best means of confirming the satisfactory operation of emergency communications and procedures. Live exercises provide the only means for fully testing the crucial arrangements for handling the media.
- Depending on the customer involved, there may be a few mandatory exercises run throughout the year by various agencies and full or partial participation in one or more of these may be helpful in rehearsing some or all the local response.

#### *1.11.3.3 Exercise Planning*

A graduated programme of exercises should be planned so that all participants have gained appropriate experience before being confronted with a live exercise. It should be noted that significant resources are required to plan and implement realistic and effective live exercises and therefore all participants should have received appropriate training to make best use of time and resources.

The more realistic an exercise, the more beneficial it is to the company and the individuals concerned. The temptation to manipulate the timing of an exercise to avoid any disruption of normal business should be avoided – a degree of disruption is inevitable and crises tend to strike at the least convenient times.

To provide the maximum value from an exercise, details of the scope and timing of the exercise should be restricted to the planning staff. The elements of surprise, uncertainty and pressure are major elements of a crisis that need to be replicated as far as possible.

#### *1.11.3.4 Post- Exercise debrief Review*

Provision should be made for objective observation of the exercise by persons from outside the Crisis Management Team. Consideration could also be given to the use of outside consultants who could give feedback at appropriate points, highlighting the repercussions of an action just taken.

The value of an exercise is in testing the crisis management planning and the performance of all individuals within the crisis management organisation. Information gathering at all stages is required to give an accurate picture of the response to events as they unfolded. Each exercise will produce lessons to be learned that may need to be incorporated in the Business Continuity Management Plan in readiness for the next exercise or a real-life crisis. The Emergency Response Team should be debriefed as soon as possible after the end of the exercise to ensure it is fresh in people's minds.

Whatever type of exercise is chosen it is important to record and evaluate the event. Provision of a succinct report of successes, failures and corrective actions to which management can refer is a vital part of the overall learning process. In the event of a crisis, previous exercise reports demonstrate to stakeholders, and any subsequent formal inquiry, the commitment of the organisation to the safety of people, property and the environment.

## 2.0 Escalation Levels

Incident Management is managed daily using the Incident Management Procedure OP-PROC-02-00-DGS. Should a disruptive event occur then the Major Incident Management Plan would come into operation.

The Major Incident Management Plan provides the management structure to respond to a major incident using personnel with the necessary responsibility, authority and competence to manage an incident.

Incidents differ in their severity and in the seriousness of their implications for DigiPlex and our customers. Escalation codes reflect five levels of severity shown in the table below. In addition, High Risk Change Management activities require notification to the Senior Leadership team so that they are aware of the changes being undertaken and be prepared should an incident occur.

### Priority Level 1—Critical: Life Safety or Catastrophic Failure Actual or Imminent IT Load Loss

Priority 1 Incident Examples	Action to be taken
<ul style="list-style-type: none"> <li>An injury that causes death or injury for which hospital admittance is necessary (for one person or more).</li> <li>A building fire for which evacuation or fire department response is necessary.</li> <li>Hazardous material released into the environment.</li> <li>A natural disaster with obvious building damage.</li> <li>Equipment failure that causes or could cause an SLA Breach to more than 1 customer</li> <li>PDU or other electrical distribution failure with IT load loss.</li> <li>One or more server racks down with IT load loss.</li> <li>UPS on battery because of a distribution failure—recovery not likely.</li> <li>UPS system on bypass—servers are on raw utility power.</li> <li>Total loss of water to the building—recovery not likely.</li> <li>Large-scale cooling system failure. IT load loss is imminent.</li> <li>An event that causes actual or imminent loss of IT load.</li> </ul>	<p>When EOPs are available and recovery is possible:</p> <ul style="list-style-type: none"> <li>Do the applicable EOPs.</li> <li>Escalate immediately to SLT</li> </ul> <p>When applicable EOPs are <i>not</i> available:</p> <ul style="list-style-type: none"> <li>Escalate immediately to SLT</li> <li>SLT activate Major Incident Plan</li> </ul>
High Risk -Change Management Examples	Announcing a Procedure in Progress
<ul style="list-style-type: none"> <li>Work that can cause catastrophic facility failure.</li> <li>Work on a live, critical system at N capacity (no redundancy).</li> </ul>	<ul style="list-style-type: none"> <li>Send a notification to SLT that describes the work to be carried out</li> </ul>

- Work on a power or cooling component that represents a single point of failure in a critical system.
- Removal of a critical control system from service.

#### Priority Level 2—High : Loss of Redundancy or System-Wide Vulnerability

Priority Level 2 Incident Examples	Action to be taken
<ul style="list-style-type: none"> <li>• An injury that results in emergency medical care, or when medical care beyond first aid is necessary for two or more persons.</li> <li>• Equipment failure that causes or could cause an SLA breach to a customer</li> <li>• Chiller failure—if the system is at N capacity.</li> <li>• Chilled water pump failure—if the system is at N capacity.</li> <li>• Loss of BMS control or monitoring to the building</li> <li>• Fire system malfunction.</li> <li>• Power transferred to generators automatically or manually.</li> </ul>	<ul style="list-style-type: none"> <li>• Do the applicable EOPs.</li> <li>• Escalate as soon as possible to SLT</li> <li>• Decision taken by CEO, Head of Operations to activate Major Incident Plan</li> </ul>
High Risk - Change Management Examples	Announcing a Procedure in Progress
<ul style="list-style-type: none"> <li>• A procedure that decreases redundancy on one or more critical systems.</li> <li>• Work related to critical environment systems that has a possible effect on the critical load.</li> </ul>	<ul style="list-style-type: none"> <li>• Send a notification alert to SLT that describes the change.</li> </ul>

#### Priority Level 3—Medium N+1 Redundancy Remains ( Business as Normal)

Priority Level 3 Incident Examples	Action to be taken
<ul style="list-style-type: none"> <li>• An injury for which medical care beyond first aid is necessary for only one person.</li> <li>• Chiller failure—if the system has N +1 or more redundancy remaining.</li> <li>• Chilled water pump failure—if the system has N +1 or more redundancy remaining.</li> <li>• Fire alarm started because of a malfunction or non-emergency issue.</li> <li>• Other events that decrease the capacity of control systems, but do not cause system failures.</li> </ul>	<ul style="list-style-type: none"> <li>• Do the applicable SOPs.</li> </ul>
Moderate Risk- Change Management Examples	Announcing a Procedure in Progress
<ul style="list-style-type: none"> <li>• Scheduled maintenance on the conditioned power distribution system.</li> <li>• Scheduled maintenance on an isolated UPS (no live load).</li> </ul>	<ul style="list-style-type: none"> <li>• No announcement needed</li> </ul>

- Large-scale work that does not jeopardize existing redundancies (N+1 or more).
- Fire system isolation.
- Other procedures that cause a reduction in control or monitoring system capacity.

#### Priority Level 4 Low: Minor Issues

Priority Level 4 Incident Examples	Action to be taken
<ul style="list-style-type: none"> <li>• An injury for which only first aid treatment is necessary.</li> <li>• Individual IEC, CRAH or CRAC issues.(Not SLA Affecting)</li> <li>• Small leaks (oil, coolant, water).</li> <li>• Filter issues.</li> </ul>	<ul style="list-style-type: none"> <li>• Do the applicable SOPs for regular maintenance or repair.</li> </ul>
Low Risk - Change Management Examples	Announcing a Procedure in Progress
<ul style="list-style-type: none"> <li>• Regular activities with minimal risk of effect on the critical load.</li> </ul>	(Not applicable)

#### Level 5 —Planned: Request

Priority Level 5 Event Examples	Action to be taken
<ul style="list-style-type: none"> <li>• Customer Request</li> <li>• Sales Opportunity</li> </ul>	<ul style="list-style-type: none"> <li>• Request Fulfillment</li> </ul>

## 3.0 Emergency Contact Information

### 3.1 Major Incident Management Team

Name	Role	Contact Number	Email
Gisle Eckhoff	CEO DigiPlex: CCOM leader	+47 922 20 008	gisle.eckhoff@digiplex.com
Dan Oldham	COO, DigiPlex	+46 72 219 36 13	doldham@digiplex.com
Halvor Bjerke	Head of Operations	+47 971 75 958	hbjerke@digiplex.com

### 3.2 Emergency Response Team

Name	Role	Contact Number	Email
Pål Rune Viken	Site Manager	+47 916 23 897	pviken@digiplex.com
Frode Elden Kay	Service Team Manager	+47 915 36 727	fekay@digiplex.com
On Call	Service Team	+47 977 17 393	No mail



### 3.3 Key Suppliers Emergency Contact Information

Name	Role	Phone Number
<b>Police</b>	Local Law Enforcement	112
<b>Fire Brigade</b>	Local Fire Brigade	110
<b>Ambulance</b>	Medical Emergency	113
<b>SCHNEIDER</b>	UPS / Breaker Vendor	+47 23191200
<b>Bostek</b>	MTU Generators	+47 55947460
<b>PonPower</b>	Pon Generators	+47 23170500
<b>Lysteknikk</b>	Electrical	+47 48000049
<b>Securitas</b>	Security	+47 02452
<b>Pingvin Klima</b>	Cooling	+47 22650415

## 4.0 Emergency Response Procedures

### 4.1 Fire

This section gives the procedures to complete before, during, and after an emergency event. It contains definitions for clarity, where necessary.

For further information see DigiPlex's Fire Procedure -**HS-PROC-03-00-DGS**

To keep fires and the damage they cause to a minimum, train personnel on basic procedures and hazard recognition.



Preparation	<ul style="list-style-type: none"> <li>✓ Identify and communicate emergency assembly areas.</li> <li>✓ Keep work areas clean to decrease potential hazards: remove flammable waste from the data centre daily, obey e-permit hot work procedures when welding or cutting.</li> <li>✓ Keep exit routes and fire extinguishers clear and free of blockages at all times.</li> <li>✓ Organize mandatory, regular fire evacuation drills for all employees, suppliers and Customers.</li> <li>✓ Weekly Walk arounds to ensure Facility maintains high standard.</li> <li>✓ Adhere to Fire Zoning and Gas Suppressions Systems</li> </ul>
Immediate Action on Discovery	<p>If you find a fire, operate the nearest manual pull alarm or immediately tell Security to start audible and visual alarms.</p> <p><u>Small Fires</u></p> <p>You can usually extinguish small fires (those contained to a small area or to equipment where flames cannot touch other flammable materials) without a full evacuation of personnel.</p> <p>Tell persons near you about the fire, get help from them, and then immediately telephone Security.</p> <p>If you are trained and can safely extinguish the fire with available resources, use the appropriate extinguisher.</p> <p><u>Large Fires</u></p> <p>If you find a large fire, start the fire alarm if it is not in operation.</p> <p>Tell Security to start audible and visual alarms.</p> <p>Go away from the area, out of the building, and to the nearest assembly area. During the evacuation, instruct other persons to go out of the building. Do not go back into the building (even if the fire alarm stops) until told to do so.</p>
Recovery Response	<ul style="list-style-type: none"> <li>• The on-site Incident Commander instructs designated personnel to speak with the fire department and give them information about location of fire and status of personnel.</li> <li>• When the fire department gives permission to go back into the building, the Incident Commander will issue the All Clear: The data centre is safe and employees can start work again.</li> <li>• When appropriate, operational or designated personnel such as members of the development team should complete a review of the <i>Site Condition</i></li> </ul>


	<ul style="list-style-type: none"> <li>• Senior Operations and Senior Leadership Team make the decision to continue operations (fully or not); start operations with caution.</li> <li>• Photograph damaged areas and repair water-, smoke- and fire-damaged equipment.</li> <li>• Organise tasks to clean the affected area, salvage operations, and resume customer services.</li> </ul>
Communication -	✓ Criss Communication Manual -CCOM-MAN-01-00-DGS



## 4.2 Bomb or Terrorist Threat

The clear majority of bomb threats are hoaxes designed to cause alarm and disruption. As well as the rare instances of valid bomb threats, terrorists may also make hoax bomb threat calls to intimidate the public, businesses and communities, to draw attention to their cause and to mislead police. While many bomb threats involve a person-to-person phone call, an increasing number are sent electronically using email or social media. Telephonic threats



**Regardless, always tell the applicable authorities when there is a threat. They will make to decision about how to respond.**

<b>Preparation</b>	<ul style="list-style-type: none"> <li>✓ Train employees what to do in an emergency.</li> <li>✓ CCTV Monitoring &amp; Access Control, Fencing</li> <li>✓ Keep work areas clean to decrease potential hazards</li> <li>✓ Daily Walk arounds to ensure Facility maintains high standard.</li> </ul> <div style="text-align: center;">  <p><b>DO NOT MOVE or TOUCH a SUSPICIOUS OBJECT</b></p> </div>
Immediate Action on Discovery	<p><b>Telephone Threats</b></p> <p>In the event of a threat being received from a caller on the telephone the following steps should be taken:</p> <ul style="list-style-type: none"> <li>✓ Stay calm and do not panic</li> <li>✓ Ask the caller to clarify their message and give as much detail as possible, specifically: <ul style="list-style-type: none"> <li>✓ where has the bomb been planted</li> <li>✓ when is it due to go off</li> <li>✓ why has it been planted</li> <li>✓ what does the device look like</li> </ul> </li> <li>✓ Every attempt should be made to keep the caller talking for as long as possible</li> <li>✓ Note as much detail as possible regarding accents, background noises etc. and complete the form at Appendix A</li> </ul>

	<ul style="list-style-type: none"> <li>✓ The details should be passed to a member of management or the security staff as soon as possible.</li> </ul> <p><b>Suspicious packages or letters</b></p> <p>The possibility exists that a suspect device could be received through the post.</p> <p>The following are potential indicators of a letter/parcel bomb:</p> <p><b>A package is Suspicious if it has more than one of</b></p> <ul style="list-style-type: none"> <li>✓ Unusually heavy for its size</li> <li>✓ Heavier on one side</li> <li>✓ A springy feel to the outer packaging</li> <li>✓ Excessive packaging</li> <li>✓ Excessive postage paid</li> <li>✓ Grease or sweat stains on outer cover</li> <li>✓ A smell of marzipan</li> <li>✓ Unusual writing or spellings</li> <li>✓ Addressed to persons by job title, e.g. 'Personal for the CEO'</li> <li>✓ Protruding wires</li> <li>✓ No return address</li> <li>✓ Immediately tell Security and management: give the location and an accurate description of the object.</li> <li>✓ Do not move, or touch the package.</li> </ul> <p> <b>Standard fire evacuation routes and assembly points will not always be appropriate</b></p> <p> <b>The fire alarm shall not be used</b></p>
Recovery Response	<ul style="list-style-type: none"> <li>• The on-site Incident Commander instructs designated personnel to speak with the Police department and give them information about location and details of device.</li> <li>• The on-site Incident Commander instructs the area to be cordoned off. Assembly must take place at least 150 metres out of the line of sight of the building. However, if there is reason to believe an explosive device is in a particular form, the following distances should be observed: <ul style="list-style-type: none"> <li><b>Briefcase - 150m</b></li> <li><b>Suitcase - 200m</b></li> <li><b>Bigger-400m</b></li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• The on-site Incident Commander decides to evacuate externally or inwardly evacuate (invacuation).</li> <li>• If it is decided to evacuate, the person responsible for each area should verbally inform all staff that there is a 'security incident' and that the area is to be vacated immediately. This must be done in a calm and orderly fashion.</li> <li>• When the Police gives permission to go back into the building, the Incident Commander will issue the All Clear: the data centre is safe and employees can start work again.</li> </ul>
Communication -	✓ Criss Communication Manual -CCOM-MAN-01-00-DGS

### 4.3 Civil Disturbance

Civil disturbance is “a civil unrest activity such as a demonstration, riot, or strike that disrupts a community and requires intervention to maintain public safety.”


Civil disturbances, or unrest, can cause a variety of subsequent issues such as violence and assault, disorderly conduct, vandalism.



**Regardless, always tell the applicable authorities when there is a threat.**

**They will make to decision about how to respond.**

<b>Preparation</b>	<ul style="list-style-type: none"> <li>✓ Train employees what to do in an emergency.</li> <li>✓ Tell Security about people acting suspiciously around perimeter fence.</li> <li>✓ Ensure that only authorised person enter through the gates.</li> <li>✓ Resolve problems between staff quickly</li> </ul>
Immediate Action on Discovery	<p><b>Internal Events</b></p> <p>In the event of an occurrence taken place within the perimeter fence the following steps should be taken:</p> <ul style="list-style-type: none"> <li>✓ Immediately tell your Manager and Security about the situation about the possible risk of work place violence.</li> <li>✓ Keep this confidential</li> <li>✓ On-Site Management will investigate and take the appropriate action.</li> </ul> <p><b>External Events</b></p> <p>In the event of an occurrence taken place outside the perimeter fence the following steps should be taken:</p> <ul style="list-style-type: none"> <li>✓ Immediately tell Security about the situation</li> <li>✓ Security will contact Police and Site Director</li> <li>✓ Stop all work outside and have everyone inside building.</li> <li>✓ Lock down building</li> <li>✓ Keep away from windows.</li> <li>✓ On-Site Management will investigate and take the appropriate action.</li> </ul>

	 <b>DO NOT GO OUTSIDE</b>
Recovery Response	<ul style="list-style-type: none"> <li>The on-site Incident Commander instructs designated personnel to speak with the Police department and give them information about location and details of device.</li> <li>The on-site Incident Commander instructs the area to be shut down. No vehicles allowed to enter or leave campus. All Personnel outside and to be brought inside quickly and the building is locked down.</li> <li>Site Personnel are to meet in central safe area away from Windows</li> <li>When the Police gives permission to go leave the area, the Incident Commander will issue the All Clear: the data centre is safe and employees can start work again.</li> </ul>
Communication -	<ul style="list-style-type: none"> <li>✓ Your immediate manager</li> <li>✓ CEO/COO- Major Incident Team Leader</li> </ul>

## 4.4 Power Outage

The Data centre is backed up by autonomous diesel driven generators and UPS systems. A full support-regime is in place which allows us to re-fill onsite diesel tanks and maintain the generators at full-load continuously, so a customer never loses power to their racks.



<b>Preparation</b>	<ul style="list-style-type: none"> <li>✓ Regularly monitor and refuel generator fuel tanks.</li> <li>✓ Regular Maintenance on Generators and monthly running checks.</li> <li>✓ Regular Maintenance on UPS systems.</li> <li>✓ Maintain EOP's and make them available to the service team call-out.</li> </ul>
Immediate Action on Discovery	<ul style="list-style-type: none"> <li>✓ Inform Site Manager of Outage and give necessary updates.</li> <li>✓ Follow lockout-tagout procedures, if necessary.</li> <li>✓ Verify Plant room equipment (Both Mechanical/ Electrical) in Operation</li> <li>✓ Examine BMS to verify that all systems are online</li> <li>✓ Look for critical equipment alarms.</li> <li>✓ Follow relevant EOP's and SOP's</li> </ul>
Recovery Response	<ul style="list-style-type: none"> <li>Communicate with Site Manager about updates on power restoration.</li> <li>Continually refill generator fuel tanks until powers restored.</li> <li>When powers restored top up generator fuel tanks.</li> </ul>
Communication -	<ul style="list-style-type: none"> <li>✓ Line Manager</li> <li>✓ CEO/COO- Major Incident Team Leader- Depending on event</li> </ul>

## 4.5 Water Incident

As far as Data centre disasters go, small amounts of water have the power to destroy machines by short-circuiting processing units, potentially leading to server room downtime and a need for swift maintenance.



<b>Preparation</b>	<ul style="list-style-type: none"> <li>✓ Monitoring of facility with automated leak detection systems.</li> <li>✓ Regular Site Walkarounds.</li> <li>✓ Regular maintenance of monitoring systems</li> </ul>
Immediate Action on Discovery	<ul style="list-style-type: none"> <li>✓ Inform Site Manager of Incident and give necessary updates.</li> <li>✓ Examine BMS to verify that all systems are online</li> <li>✓ Isolate Leak / Water Incident.</li> </ul>
Recovery Response	<ul style="list-style-type: none"> <li>✓ Communicate with Site Manager about updates on the Water Incident and restoration.</li> <li>✓ Contact Suppliers to Carry out repair</li> <li>✓ Cooling Unit Failure – Seek specialist support</li> </ul>
Communication -	<ul style="list-style-type: none"> <li>✓ Line Manager</li> <li>✓ CEO/COO- Major Incident Team Leader- Depending on event</li> </ul>

## 4.6 Severe Weather

Severe weather is best defined as weather conditions in the borderline or outside the local norm for what buildings and plant are designed for.

Typical for Oslo-area will be events with wind, rain, snow, lightning, extreme temperatures of the season. One of these or any combination.



Preparation	<ul style="list-style-type: none"> <li>✓ Pay attention to weather forecasts and warnings.</li> <li>✓ Always keep outside areas tidy to decrease potential flying debris and amount of combustible items close to the building.</li> <li>✓ Inspect and maintain water drains and weather sealing regularly.</li> </ul>
Immediate Action on Discovery	<ul style="list-style-type: none"> <li>✓ Prepare for the weather that have been forecasted, or what you observe as oncoming.</li> <li>✓ Top up diesel tanks to have full capacity, if timing allows.</li> <li>✓ Execute backout plans if weather sensitive operations are in progress, like craning, outside works etc.</li> <li>✓ Serviceteam must focus on plant operations and inspect exposed areas regularly. Be prepared for power outage and other relevant EOP's</li> <li>✓ Plan ahead depending on the outlook and expected duration of event.</li> </ul>
Recovery Response	<ul style="list-style-type: none"> <li>✓ Action will depend on the events unfolding. Action as required to protect life and assets.</li> <li>✓ Photograph damaged areas and repair damaged equipment.</li> <li>✓ Organise tasks to clean the affected area, salvage operations, and resume customer services.</li> <li>✓ Continue to listen to a Weather Radio or to local radio stations for updated information or instructions, as access to roads or some parts of the community may be blocked.</li> </ul>
Communication -	<ul style="list-style-type: none"> <li>✓ CEO/COO- Major Incident Team Leader</li> <li>✓ Site Manager</li> </ul>



## 4.8 Hazardous Material Spill

Most hazardous Material spills that can occur in our data centre environment are classified as an Incident, and on-site trained personnel can respond to them. The level of response depends on the quality and type of material that has escaped. If there is a hazardous material spill from UPS Battery Banks, diesel fuel tanks, diesel refuelling or critical infrastructure such as generators, chillers or transformers .Hazardous assessment have been undertaken under the Hazardous Substances procedure HS-PROC-02-00-DGS.



The following information is a reminder of the Environmental Emergency Control Procedure, ENV-PROC-03-00-DGS.

Preparation	<ul style="list-style-type: none"> <li>✓ Keep sufficient chemical-spill response supplies at all times and in a practical distance to the equipment that contains hazardous materials.</li> <li>✓ Regularly check equipment is available</li> <li>✓ No Hazardous Material to be stored on site without DigiPlex's Permission</li> <li>✓ Hazardous Material to be stored in bunded containers.</li> <li>✓ All Hazardous substances are correctly labelled</li> <li>✓ All Hazardous Material must have a material safety data sheet (MSDS) is available for each chemical that is used, processed, and kept on site.</li> <li>✓ All Hazardous Materials over 10 litres to be assessed by Management</li> <li>✓ Management must make sure that all combustible and flammable materials are kept in appropriate containers or cabinets.</li> <li>✓ Train personnel regularly on spill response.</li> <li>✓ Regular audits from QA &amp; compliance depart and Safety Representatives.</li> </ul>
Immediate Action on Discovery	<ul style="list-style-type: none"> <li>✓ Notify On-site Security or site operations team.</li> <li>✓ Security to notify Site Operations Team.</li> <li>✓ Emergency Response team attend spill.</li> </ul> <p>The three significant hazardous material spills are UPS, diesel fuel and critical Infrastructure equipment</p> <p><b>UPS</b>—<i>Identify the source of the leak and stop the flow of material:</i></p> <ul style="list-style-type: none"> <li>Use a battery acid spill response kit.</li> <li>Use appropriate PPE (such as acid-resistant gloves, an apron, sleeves, boots, and a face shield).</li> <li>Store Hazardous waste safely</li> <li>Disposal for Hazardous Waste through specialist waste supplier</li> <li>Replace and decontaminate all materials you used in the spill response.</li> </ul> <p><b>Diesel Fuel Tanks/ Refuelling</b> –<i>Extinguish all sources of ignition:</i></p> <ul style="list-style-type: none"> <li>Try to stop the spill at the source (for example, close valves or stop leaks).</li> <li>Tell the Site Manager of the spill.</li> </ul>

	<p>If possible, contain the material before it is released out of the emergency generator pad/ refueling area.</p> <p>Use absorbent materials and make emergency trenches with non-sparking shovels and brooms.</p> <p>Activate Specialist Clean up supplier</p> <p>Put covers over nearby storm drains.</p> <p>Stop the flow and clean the spilled materials.</p> <p>The Site Manager / Head of Operations together with the CEO/COO will speak with external agencies as appropriate.</p> <p>Store Hazardous waste safely</p> <p>Disposal for Hazardous Waste through specialist waste supplier</p> <p>Replace and decontaminate all materials you used in the spill response.</p> <p><b>Critical Infrastructure Equipment</b>—When you find a release of antifreeze (Glycol) or coolant, motor or lube oil, or hydraulic fluid from operating equipment, use the action items described in the previous section on diesel fuel tanks /refuelling above.</p>
Recovery Response	<ul style="list-style-type: none"> <li>• Photograph damaged areas and repair damaged equipment.</li> <li>• Organise tasks to clean the affected area,</li> <li>• Liaise with relevant authorities if required</li> </ul>
Communication -	<ul style="list-style-type: none"> <li>✓ CEO/COO- Major Incident Team Leader</li> <li>✓ Line Manager</li> <li>✓ Key Suppliers</li> </ul>

## 4.9 Cooling Failure

The Data center has closed cooling systems supported by power system. Conditioned modules are supported by redundant chillers feeding in-module redundant close control units.

<b>Preparation</b>	<ul style="list-style-type: none"> <li>✓ Regularly monitor and refuel generator fuel tanks</li> <li>✓ Regular maintenance of site equipment.</li> <li>✓ Automated monitoring and messaging on abnormalities.</li> <li>✓ Regular inspections done by onsite staff in all areas.</li> </ul>
Immediate Action on Discovery	<ul style="list-style-type: none"> <li>✓ Inform Site Manager of Outage and give necessary updates.</li> <li>✓ Examine BMS to verify that all systems are online</li> <li>✓ Look for critical equipment alarms.</li> </ul>
Recovery Response	<ul style="list-style-type: none"> <li>• Communicate with Head of Operations about updates on Cooling restoration.</li> <li>• See Power Outage Emergency Response Plan for power failure.</li> <li>• Water Leak - Seek specialist support</li> <li>• Colling Unit Failure – Seek specialist support</li> </ul>
Communication -	<ul style="list-style-type: none"> <li>✓ Line Manager</li> <li>✓ CEO/COO- Major Incident Team Leader- Depending on event</li> </ul>

## 5.0 Appendices

**Appendix 1 Bomb Threat Checklist**

**Appendix 2 Event Log**

**Appendix 3 Crisis Review/ Debrief Form**

## Appendix 1 Bomb Threat Checklist

In you receive a bomb threat, remain calm and record the information listed below. Remember that over 90% of such calls are hoaxes, but they should always be treated seriously. Do not be afraid to ask the questions suggested here, but do not interrupt the caller or say anything to antagonise him or her.

**Date:**

**Time:**

**Operator:**

**Exact Words of Caller:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

### Details of Caller

**Phone Type:**

**Call Box**

**Mobile**

**Landline**

**Caller:**

**Man**

**Woman**

**Old**

**Young**

**Speech:**

**Accent**

**Serious**

**Laughing**

**Rational**

**Rambling**

**Intoxicated**

**Nervous**

**Did the message sound spontaneous or pre-written and read out?**

### Background noises

**Did you hear any noise in the background?**

**Traffic**

**Talking**

**Typing**

**Machinery**

**Airport**

**Music**

**Children**

**Other (specify) \_\_\_\_\_**

### Questions to ask

**1. Where is the bomb planted?**

**2. When is the bomb due to go off?**

**3. Describe the bomb to me.**

**4. Why are you doing this?**

**Note Of caller line identifier:**

**This information must be passed immediately to Security or a Manager.**

Document Number:  
BCP-MAN-01-00-DNAS &  
DRAS

Revision:  
A

Issue Date:  
September 2018

Owner  
Site Manager



## Appendix 2 Event Log

EVENT LOG					
Time	Message		Information	Action	Initials
	From	To			

### Appendix 3 Crisis Review/ Debrief Form

The Crisis review/ debrief form helps the team to discuss lessons learned. This is the last step before the crisis can be closed. The purpose is to identify what we did correctly and how we can improve.

<b>Participants</b>		<b>Facilitator</b>	
<b>Event</b>		<b>Date of the Event</b>	
<b>Overall Assessment</b>			
<b>Lessons Learned</b>			
<b>Action Identified</b>	<b>Task</b>	<b>Assigned to</b>	<b>Target Date</b>