DigiPlex's Major Incident Plan

Managing and Recovering from Major Incidents

Contents

1.0 Introduction

Many problems are dealt with on a day-to-day basis, but a major disruption could come from different sources, any of which could damage DigiPlex.

The potential commonly occurring disruptions that could happen:

- Customer Outage
- Sabotage attack on our Customers
- Loss of critical equipment / IT / telecommunications
- Loss of utility (power, water)
- Denial of site or structural damage (e.g. fire, natural disaster)
- Supply chain disruption.
- Loss of staff and key skills, either temporarily or permanently (e.g. flu, weather, health and safety incidents)

2.0 Aim of the Major Incident Plan (MIP)

2.1 Purpose of the MIP

The purpose of the Major Incident Plan is to increase resilience for the critical activities of DigiPlex at the time of a major incident or disaster. The MIP is written to deal with generic hazards and threats and to enable DigiPlex to perform its functions in relation to a wide range of possible scenarios eg flood, act of terrorism, loss of building(s), loss of staff, loss of services (power, water) etc. The primary purpose in dealing with a major incident is, immediately, to ensure the safety and well-being of DigiPlex's staff/customers/ and supply chain and, thereafter, to ensure recovery as early as possible from the effects of the incident.

Critical activities identified for DigiPlex:

- An injury that causes death or injury for which hospital admittance is necessary (for one person or more).
- A building fire for which evacuation or fire department response is necessary.
- Hazardous material released into the environment.
- A natural disaster with obvious building damage.
- Equipment failure that causes or could cause an SLA Breach to more than 1 customer
- PDU or other electrical distribution failure with IT load loss.
- One or more server racks down with IT load loss.
- UPS on battery because of a distribution failure–recovery not likely.
- UPS system on bypass–servers are on raw utility power.
- Total loss of water to the building–recovery not likely.
- Large-scale cooling system failure. IT load loss is imminent.
- An event that causes actual or imminent loss of IT load

In addition to the specific requirements of each activity, all the activities are dependent on DigiPlex's ability to provide common core infrastructure and process support involving dependencies on key personnel and organisations internal and external to DigiPlex.

2.2 DigiPlex's Major Incident Team (MIT)

DigiPlex's Major Incident Team is responsible for the initial evaluation and the overall handling within DigiPlex of a major emergency, incident or threat. The CEO is Convenor of the Major Incident Team. In his absence, the COO will act as Convenor.

The following personnel form the Major Incident Team

- CEO- Chair
- COO- Deputy
- CCO
- CSMO
- CDO
- FD
- HR Director
- Head of Operations
- IT Director
- PA CEO -Secretary

3.0 Activation of the Major Incident Plan (MIP)

If an incident occurs on a site, attempts to manage the incident locally will be enacted in the first instance. The incident should be initially reported via existing mechanisms (e.g. Security, Telephone).

Should these attempts not resolve the issue, the most Senior Member of Staff from the affected area (as designated in Site Business Continuity Plans and Emergency Response Procedures) is to contact the persons identified in 2.1 above.

4.0 Incident Definitions and Assessment Criteria

4.1 Incident Assessment

Find out **the basics**: the who, what, why, where, when and how (5 'W's' and H). **Form 3** should be used to document these. The following aspects should be included in the early incident assessment:

- Expected duration of the acute phase of the incident:
- Health and safety: Impact on people (welfare, transport)
- Ascertain whether critical staff members are available
- Establish whether additional members of suitably skilled employees can be redeployed
- Could additional short-term staff help – are call-out lists of any use? - Liaise with temporary staffing (and then alternative providers) for the provision of temporary staffing resources
- Impact on buildings and property (accessibility, status, critical systems, security, cordons):
- Impact on IT and communications (critical systems, network, telephony, communications):
- Impact on operations (process peaks, resources, rooms)
- Possible future outcomes.

Consider the need to ascertain and implement **alternative systems** (e.g. IT, telephones, use of hand-held radios, runners). If appropriate, reassign work tasks accordingly or redeploy temporarily

- Think – who needs to know about the disruption – communicate it – which areas have priority?
- Can non-affected areas have a re-designated function for essential functions?
- Could other services (e.g. local authority, police, fire and rescue) help?
- How soon could suppliers help? Are there alternative suppliers?

Long-scale incidents, including pandemic and other large-scale infectious disease activity, will demand the answer to large-scale management questions:

- Can we keep all activities going?
- Have we got the resources?
- How soon can we get back to normal?

Any given situation may require two types of response – a less flexible and more rehearsed mode for those elements which are more fixed and predictable, and a more flexible approach for less predictable or novel elements.

4.2 Criteria for activation of the plan

The following criteria shows when to activate this plan

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

Level 1 Incident Examples	Action to be taken
• An injury that causes death or injury for which hospital admittance is necessary (for one person or more). • A building fire for which evacuation or fire department response is necessary. • Hazardous material released into the environment. • A natural disaster with obvious building damage. • Equipment failure that causes or could cause an SLA Breach to more than 1 customer • PDU or other electrical distribution failure with IT load loss. • One or more server racks down with IT load loss. • UPS on battery because of a distribution failure–recovery not likely. • UPS system on bypass–servers are on raw utility power. • Total loss of water to the building–recovery not likely. • Large-scale cooling system failure. IT load loss is imminent. • An event that causes actual or imminent loss of IT load.	When EOPs are available and recovery is possible: Do the applicable EOPs. Escalate immediately to SLT When applicable EOPs are *not* available: Escalate immediately to SLT SLT activate Major Incident Plan . .
High Risk Change Management Examples	**Announcing a Procedure in Progress**
• Work that can cause catastrophic facility failure. • Work on a live, critical system at N capacity (no redundancy). • 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.	• Send a notification to SLT that describes the work to be carried out

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

Level 2 Incident Examples	Action to be taken
• An injury that results in emergency medical care, or when medical care beyond first aid is necessary for two or more persons. • Equipment failure that causes or could cause an SLA breach to a customer • Chiller failure–if the system is at N capacity. • Chilled water pump failure–if the system is at N capacity. • Loss of BMS control or monitoring to the building • Fire system malfunction. • Power transferred to generators automatically or manually.	• Do the applicable EOPs. • Escalate as soon as possible to SLT • Decision taken by CEO, Head of Operations to activate Major Incident Plan
High Risk Change Management Examples	**Announcing a Procedure in Progress**
• A procedure that decreases redundancy on one or more critical systems. • Work related to critical environment systems that has a possible effect on the critical load.	• Send a notification to CEO & Head of Operations that describes the change.

5.0 Major Incident Control Room

Following the decision to activate the MIP, the MIT secretary will identify a meeting room to establish the MIT. Any meetings in place using the room will be immediately terminated.
The Major Incident Bridge Facility will be initiated in Goto meet.

6.0 Initial MIT Meeting Agenda

The minutes and actions of the initial meeting to be recorded USING FORM 1.
Suggested Agenda

1. Allocation of MIT roles and responsibilities
RECORD USING FORM 2

- Confirm the membership of the MIT.
- Assign individuals to roles.
- Ensure individuals understand the role to which they have been assigned.
- Ensure individuals review and update their own Action Plan.

2. Initial incident assessment and analysis of the situation
RECORD USING FORM 3

- Examine the scope of the issue and potential implications.
- Scrutinise incident updates and scale of damage.
- Evaluate short-term impact of the incident.
- Ascertain what support mechanisms may be needed for all stakeholders and when access to the incident site may be available.

3. Confirm ownership of the incident

- Is the incident of sufficient impact or potential impact to require full MIT involvement.

4. Define objectives of the MIT
RECORD USING FORM 4

- What are the priorities at this time?
- What parameters and constraints does the MIT need to work within?
- What are the possible long-term effects of the incident?
- Determine MIT objectives to align with above.

5. Develop a response strategy
RECORD USING FORM 5

A number of strategies may emerge during the initial stages, but agreement has to be reached on determining the most appropriate to adopt. Updates from the Communications Team will be important, as will the agreement and approval of press statements and releases. Recommendations for reallocation and relocation should be considered.

6. Agree actions arising and next meeting

Actions will be based on the adopted strategy and the MIT Action Checklists.
The checklists may also be used to record some of the key actions taken. The MIT may decide to arrange meetings of smaller sub-sets of people which may happen prior to the next full MIT meeting.
Determine the schedule of meetings and roster for Major Incident Team and the time and date of the next meeting.

7.0 Subsequent Meetings of the Major Incident Team

Depending on the scale of the incident, the MIT should consider asking a Liaison Officer from the emergency services to join the Team in the Control Room. During the first few days following a major incident the Team will assemble at the Control Room (or elsewhere) at 8.00 am unless otherwise agreed. The agenda for the meetings (to be issued by the Secretary) should be:

(1) Receiving a status report of eg. Injuries, Cause, Damage, Possible further damage/-containment, Business impact assessment

(2) Examination of the scope of the issue and potential implications and review objectives of MIT. Are priorities right? Have parameters and constraints changed?

(3) Actions to manage damage including need for any specialist assistance?

(4) Actions required on Public Relations and Communications (Internal and External)

(5) Actions for Business Continuity including outline assessment of additional space requirements and identification of any additional personnel required for business continuity purposes

(6) Review the response strategy

(7) Agree new actions and next meeting.

8.0 Records of Events and Closure Report

8.1 Records of Events

Where possible the events are recorded through the ServiceNow as a Problem candidate and investigated further to establish root cause and track any lessons learnt.

8.2 Closure Report

The following should be provided as part of the Closure report:

- Background
- Description of the Incident including, if relevant the timeline
- Description of the Recovery procedures
- Description of the Communications process
- Services Affected by the Incident: duration and number of people affected
- Statement on Lessons Learned: Issue, Actions taken, Lesson Learned, Outstanding Actions

9.0 Forms

Form 1- Initial MIT Meeting Record

The Initial MIT Meeting was conducted on (date/time) ……..

Attendance - Tick

CEO -Chair		COO- Deputy	
Head of Operations		CDO	
HR		FD	
CCO		CSMO	
IT Director			

Agenda	Notes
1 Initial Assessment	
2 Confirm Ownership	
3 Define Objectives	
4 Allocation of Responsibilities	
5 Response Strategy	
6. Agree Actions	

Action	Owner	Priority or Timescale

Action	Owner	Priority or Timescale

Form 2 MIT Assigned Roles

MIT assigned Roles and Specialist/ Support Roles

Role	Description	Primary Lead	Person Assigned
MIT Lead	Responsible for all actions of the MIT in fulfilling their objectives and to maintain overall executive control and co-ordinate actions	CEO	
Finance Lead	Responsible for all financial aspects of business recovery continuity and for the financial planning aspects for establishing business recovery.	FD	
Customer Lead	Responsible for communicating with customers	CCO	
Communications Lead	Responsible for all information releases and to manage internal communications. Also to monitor press/media coverage and take action as required	CSMO	
Operations Lead	Responsible for all infrastructure issues and checking the damaged location, dealing with Security and the Emergency Services and ensure welfare of individuals eg basic facilities, water, hot food	Head of Operations	
IT Lead	Responsible for all aspects involving Information Technology or Information Services.	IT Director	
MIT Secretary	**Coordinate all administration functions for the MIT**	PA to CEO	
Other as needed			

Form 3– Incident Assessment Record

Brief summary of Information available

May Include

People Status (Causalities etc)
Health and Safety
Building and Property Status
Business Operations Status
Security Status
Details of Emergency Service Cordons
IT & Communications Status
Possible Outcomes

Additional Information Obtained

May Include:

Emergency Service Contacts
Current Operational Issues
Regulatory Requirements
Financial considerations

Source of Information:

Form 3 – Incident Assessment Record

Expected duration of the acute phase of the incident
Health and Safety
Impact on People
Impact on buildings and property (security, cordons)
Impact on IT and Communications (network, telephony)
Impact on business operations
Impact on customers
Possible future outcomes

Form 4 -MIT Objectives

Core Objectives

The following objectives are the core MIT objectives that will be applied to any major incident. Depending on the type of incident however these should be reviewed to ensure they are prioritised appropriately and specific details applied where necessary. The form should be reviewed throughout the incident to ensure they are still appropriate and therefore driving the right thinking and actions. The core objectives are to:

1. Ensure the wellbeing of staff, suppliers and customers
2. Minimise disruption and loss to customer
3. Maintain the DigiPlex's reputation.
4. Secure assets and infrastructure
5. Inform stakeholders

Ensure objectives are **S**pecific, **M**easurable, **A**chievable, **R**ealistic and **T**ime framed.		
#	**Objective**	**Deadline**
1		
2		
3		
4		
5		
6		

If possible, place in a visible position on the wall, flipchart or whiteboard.

Form 5 – Incident Response Strategy

Options available to the MIT

Insert a description of available strategic response options, together with commentary regarding the benefits and drawbacks of each.

#	Description
1	

Benefits	Drawbacks

#	Description
2	

Benefits	Drawbacks

#	Description
3	

Benefits	Drawbacks

Selected Incident Response Strategy

Based upon the information available to the MIT the following recovery strategy will be initiated:
