

Business Continuity Policy

**Commercial in Confidence / General Circulation / Redacted Version**

|  |
| --- |
| Version History |
| Version No | Version Date | Author | Summary of Changes |
| 1.0 | 02/12/13 | MH | First Issue |
| 2.0 | 14/01/14 | MH | Director and IT Director version |
| 3.0 | 11/09/19 | MH | Update to Scope |
| 4.0 | 09/1/20 | MH | Format Changes |
| 5.0 | 06/01/21 | IMcG | Changes to the Policy Key Principles |
| 6.0 | 21/09/21 | IMcG | Changes to the Incident Management  |

|  |
| --- |
| Approvals  |
| Name | Title | Date of Approval |
| Matt Harper  | ICT Director | 02/12/13 |
| Matt Harper | ICT Director | 14/01/14 |
| Matt Harper | ICT Director | 11/09/19 |
| Matt Harper  | ICT Director | 09/01/20 |
| Matt Harper  | ICT Director | 06/01/21 |
| Matt Harper  | ICT Director | 21/09/21 |

|  |
| --- |
| Distribution |
| Audience | Date of Issue | Version Number |
| Public | 02/12/13 | 1.0 |
| Public | 14/01/14 | 2.0 |
| Public | 11/09/19 | 3.0 |
| Public | 09/01/20 | 4.0 |
| Public  | 06/01/21 | 5.0 |
| Public  | 21/09/21 | 6.0 |

Contents

[Purpose 5](#_Toc31034201)

[1.0 Scope and Objectives 6](#_Toc31034202)

[2.0 Responsibilities 6](#_Toc31034203)

[3.0 Definitions 8](#_Toc31034204)

[4.0 Policy Key Principles 9](#_Toc31034205)

[5.0 Plan Activation Procedure 9](#_Toc31034206)

[Planning Scenarios 9](#_Toc31034207)

[5.3.1 Limited or no access to the building: 10](#_Toc31034208)

[5.3.2 Loss of data communications, e.g. WAN, routers, firewalls 10](#_Toc31034209)

[5.3.3 Loss of technology 11](#_Toc31034210)

[5.3.4 Loss of people, e.g. illness or death 11](#_Toc31034211)

[6.0 Assumptions 11](#_Toc31034212)

[7.0 Incident Response and Management 12](#_Toc31034213)

[Logical Sequence of Events 12](#_Toc31034214)

[Incident Management Team Structure 14](#_Toc31034215)

[7.2.1 Incident Management Team 14](#_Toc31034216)

[8.0 Notification, Escalation and Declaration 15](#_Toc31034217)

[Introduction 15](#_Toc31034218)

[Notification Process Overview 15](#_Toc31034219)

[8.2.1 Initial Notification 15](#_Toc31034220)

[Notification Process (Emergencies ONLY) 16](#_Toc31034221)

[Incident Response Assembly Locations 16](#_Toc31034222)

[8.4.1 Erith House Assembly Location 16](#_Toc31034223)

[8.4.2 Anchor Bay Wharf Assembly Location 16](#_Toc31034224)

[Escalation Process (Emergencies ONLY) 16](#_Toc31034225)

[Plan Authorisation and Declaration 16](#_Toc31034226)

[Declaration Process (Emergencies ONLY) 17](#_Toc31034227)

[9.0 Incident Response Checklists 18](#_Toc31034228)

[9.1 Key Personnel Contact Lists 18](#_Toc31034229)

[9.2 Key Suppliers (Purchasing) – Erith Group 21](#_Toc31034230)

[9.4 Key Suppliers (ICT) 21](#_Toc31034231)

[9.5 Utilities and Regulators 21](#_Toc31034232)

[Key Suppliers (Bankers) 22](#_Toc31034233)

[Passwords 22](#_Toc31034234)

[10.0 Team Responsibilities 23](#_Toc31034235)

[Initial Incident Management Team Meeting 23](#_Toc31034236)

[Incident Management Team Checklist 24](#_Toc31034237)

[Incident Manager Task Checklist 25](#_Toc31034238)

[Incident Response Recommended Actions 25](#_Toc31034239)

[Actions following a disaster declaration 26](#_Toc31034240)

[Communications Officer Task Checklist 27](#_Toc31034241)

[Safety Officer Task Check List 27](#_Toc31034242)

[Planning Team Task Checklist 27](#_Toc31034243)

[Finance and Administration Task Checklist 28](#_Toc31034244)

[Pre Incident Preparation 28](#_Toc31034245)

[Actions following an incident and prior to disaster declaration 28](#_Toc31034246)

[Actions during and after the disaster 28](#_Toc31034247)

# Purpose

This is a corporate policy that affects all Group employees and defines the procedures that shall be adopted to protect the Business in the event of an incident or other scenario that affects the normal continuation of the Business.

Any incident, large or small, whether natural, accidental, or deliberate, can cause major disruption to the Business. This document will help to ensure that the areas considered to be critical to the normal continuation of the Business following an incident will be returned to functional normality as quickly as possible.

Information contained within this document is privileged and should remain confidential to the Executive Board, Operations Board and the ICT Director, and following invocation, any whom are assigned to a Recovery Team.

There are six steps that make up the BCM lifecycle, as depicted in the diagram below:

****

**Step 1:** BCM Programme Management

**Step 2:** Understanding the Erith Group’s organisation

**Step 3:** Determining BCM Strategy

**Step 4:** Developing and Implementing BCM Response

**Step 5:** Exercising, Maintaining and Reviewing BCM arrangements.

**Step 6**: Embedding BCM in the Group’s Culture

Effective programme management ensures that BCM capability is established and maintained within the Business. This policy has the support of the Board and, depending upon the nature of the scenario, an Incident Controller will be assigned at the outset to facilitate continuity.

The policy will receive regular updates and will reflect changes in the Business and its associated people, assets, processes and technology.

# 1.0 Scope and Objectives

|  |  |  |
| --- | --- | --- |
|  | 1.1 | The Policy will be developed by the ICT Director and laterally with operational and Divisional leadership.  |
|  | 1.2 | A controlled copy of the Business Continuity Policy will be made available to all staff to enable them to have immediate access to the process and to ensure that responsibilities are known. |
|  | 1.3 | This policy applies to all companies within the Group, namely:* Erith Contractors Ltd
* Erith Haulage Ltd
* Swanton Consulting Ltd
* Erith Plant Services Ltd
* Erith Business Solutions
* Erith Holdings Ltd
 |
|  | 1.4 | The purpose of the Business Continuity Policy is to prepare the Group to be agile to respond to and recover from a disruption. |
|  | 1.5 | The objectives of the Policy are as follows: * To list the critical functions in priority order for recovery
* To detail the activation procedures and roles and responsibilities for staff
* To detail the agreed response actions following a disruption
 |
|  | 1.6 | The plan is designed to minimise operational and financial impacts of such a disaster. |

|  |
| --- |
| 2.0 Responsibilities |
|  |  |  |
|  | 2.1 | Primary responsibility for invoking the Business Continuity Policy arrangements lies with any one of the following:* Chairman
* Executive Board of Directors and Operations Board Members
* ICT Director (with the prior knowledge of the Executive Board of Directors)
 |
|  | 2.2 | Whoever invokes the Business Continuity Policy will assign an Incident Controller to manage the process of returning the Business to full functionality. They can also assign themselves the Incident Controller role. |
|  | 2.3 | Where required, all staff will comply with the requirements and instructions of the Incident Controller to recover the Business to full functionality within the shortest possible time. |
|  | 2.4 | The Business Continuity Policy shall be maintained on an ongoing basis, by the ICT Director, in conjunction with other departmental leaders and Directors, to ensure that it continues to remain fit for purpose. |
|  | 2.5 | It is the responsibility of the ICT Director to test the Policy annually to check for weakness and to ensure that it continues to remain robust and covers the eventualities identified in the Risk Register (RR). |
| 3.0 Definitions***Erith Group*** (“The **Organisation**”) is a collection of companies that lie under the Erith umbrella. All these companies are referred to as the Erith Group. For the purposes of this document the companies within the Erith Group are known as, Erith Contractors Ltd, Erith Haulage Company Ltd, Erith Business Solutions Ltd, Erith Training Services Ltd, Swanton Consulting Ltd and Erith Plant Services Ltd‘**Incident’** or ‘**Disaster’** is defined as any scenario that may interfere with the normal day to day operation of the Business.**Trigger Event** is defined as any type incident that can cause disruption. Examples of trigger events may include (but are not limited to) Fire, Data Loss, Theft, Water Ingress, Loss of a building, Sabotage, Inclement Weather, Terrorist Activities**Business Continuity Management** (BCM) is defined as the “capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident and defines a framework for identifying the organisation's risk of exposure to internal and external threats. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management, contingency planning, and data loss.**Incident Controller** means an officer responsible for **incident** activities including the development and implementation of strategic decisions and for approving the ordering and releasing of resources. **Incident Recovery** is an organised approach to addressing and managing the aftermath of a security breach, cyberattack, computer incident, security incident or operational incident.**Executive Board** is defined as the group of Officers empowered to oversee activities and strategic financial planning and decision making within the Erith Group of companies[**Operations Board**](https://www.lawinsider.com/dictionary/operations-board)is defined as the board composed of Operations Directors and Senior Managers representing their respective jurisdictions who will provide oversight and support to the Executive Board on matters pertaining to the direction of service delivery within the business, focusing on the routine, day-to-day operations of the **Organisation.****Risk Register** is defined as the controlled list of risks identified as being a threat to the normal operation of the business**Professional Staff** are defined as any employees engaged in work predominantly intellectual and varied in character as opposed to routine mental, manual, mechanical, or physical work.**Line of Business Applications** are defined as the set of critical computer applications that are vital to the running of the Erith Group. These include COINS (financials), EZone (CRM and Document Control), Office 365 suite (productivity and voice communications) |
| 4.0 Policy Key Principles |
|  | 4.1 | A Business Impact Analysis will have been performed during the identification of the Risks on the Risk Register (RR). |
|  | 4.2 | The Incident Controller is ultimately responsible for ensuring the recovery of the Business. Wherever an aspect of recovery requires spend or capex approval, the Incident Controller will liaise with an Executive Board member beforehand and register the request within his/her Recovery Report. |
|  | 4.3 | Poor practice operationally may increase the likelihood of the invocation of the Business Continuity Policy. Wherever possible, the Company’s processes and practices should prevent the need to invoke the Business Continuity Policy. |
|  | 4.4 | Data and information may be put at risk by poor education and training, misuse, and the breach of security controls. |
|  | 4.5 | The Risk Register (RR) will evolve constantly and the ICT Director will maintain the controlled register of risks to the business. The Business Impact Analysis performed for each identified risk is used to create the impact, likelihood and risk this is all documented in the Risk Analysis Framework.  |
|  | 4.6 | The Recovery of the Business will be documented in its entirety by the Incident Controller, capturing cost and time information relating to the recovery of services to the business. |
|  | 4.7 | **In the event of the disaster affecting the General Public, the Incident Controller will assign someone to talk to the press. To limit reputational damage, only pre-prepared statements should be released which are worded carefully. Telephone calls should be redirected to the Incident Controller, who will handle them accordingly. Nobody other than the Incident Controller, in conjunction with the Executive Board, is authorised to communicate on behalf of the Business.** |
| 5.0 Plan Activation Procedure |
|  | 5.1 | The plan can be activated by anybody shown at 2.1 |
|  | 5.2 | *(Section Removed)* |
|  | 5.3 | 0BPlanning ScenariosThis Policy was developed to respond to an incident that could render any or part of the Group or its locations out of service or inaccessible. In addition, it is designed to respond to situations other than the scenarios above, which may include* No access to buildings or floors at a specific location;
* Loss of data communications and the network infrastructure;
* Loss of technology;
* Loss of Professional Staff (eg in the event of a pandemic virus);
* Loss of critical plant, vehicles or machinery, whether related to a major incident or not;
* Loss of data or breach of access controls.
 |
|  |  | 24B5.3.1 Limited or no access to the building:Any incident that renders a location either totally inaccessible/unusable or partially accessible to its occupants.This scenario could produce one of more of the following impacts:* Loss of the business location or the location is rendered inaccessible.
* Loss of access to selected workspace areas, such as the floors of a building affected by water ingress or fire
* New equipment or facilities must be acquired
* Incident Management and recovery actions must be implemented
* Event causes business interruption
 |
|  |  | 25B5.3.2 Loss of data communications, e.g. WAN, routers, firewallsAny incident that disables or destroys the WAN0F[[1]](#footnote-2) / MPLS1F[[2]](#footnote-3) / IPSec2F[[3]](#footnote-4) / SDWan3F[[4]](#footnote-5) infrastructure and its communications capabilities, with a potentially disruptive effect on business operations.This scenario could produce one or more of the following impacts:* Loss of access to the WAN
* Loss of access to the Internet and line of business applications
* Incident is declared and incident recovery actions are implemented
* Use of recovery strategies, possibly other Group locations which are unaffected by the scenario, and/or manual operations as a temporary measure.
* Need for replacement facilities or equipment
 |
|  |  | 5.3.3 Loss of technology*(Erith House and Anchor Bay Wharf Communications Rooms / Network Services / Level 3 Data centre, Goswell Road)*Any incident that disables or destroys the entire Communications Room facility or its processing capability located either at Erith House, Anchor Bay, Farringdon or Goswell Road data centre, with a potentially disruptive effect on business operations.This scenario could produce one or more of the following impacts:* Loss of the use of the Communications Room and communications facilities
* Loss of the use of both Voice and Data communications services
* Incident is declared and incident recovery actions are implemented
* Use of recovery strategies, possibly other Group locations which are unaffected by the scenario, and/or manual operations as a temporary measure.
* Need for new facilities or equipment.
 |
|  |  | 26B5.3.4 Loss of people, e.g. illness or deathAny incident that disables or renders the professional staff within the Group unable to perform normal business functions, with an aggregated negative effect on business operations.This scenario could produce one or more of the following impacts:* No impact to building access or technology infrastructure
* Lack of business leadership and core management
* Insufficient professional staff to perform minimal business operations
* Lack of suitably cross-trained staff
* Need for temporary staff
 |
| 6.0 AssumptionsThe Policy has been developed and is to be maintained based on the following assumptions: |
|  | 6.1 | A complete interruption of the Business at any of its operating locations has occurred, and there is no access to the office, site, critical equipment, or business data. |
|  | 6.2 | A partial or total loss of professional staff has occurred due to employee illness resulting from a disaster, whether natural or man-made, and only a limited number of healthy employees are available to continue normal business operations. |
|  | 6.3 | Recovery from anything less than a complete interruption will be achieved by using appropriate portions of this plan. |
|  | 6.4 | Sufficient staff with adequate knowledge will be available to facilitate recovery. |

|  |
| --- |
| 7.0 Incident Response and Management |
|  | 7.1 | 1BLogical Sequence of EventsThe following checklist describes the recommended emergency response: |
|  |  | Incident Occurs |[ ]
|  |  | First person to observe the incident follows local emergency procedures and notifies the Director responsible for that particular location. If required, the first person should notify the emergency services and initiate evacuation of the building.  |[ ]
|  |  | The local Director will investigate the incident, and will determine whether an Incident Management Team (IMT) needs to be assembled (see 7.2.1). The Director will alert his colleagues on the Board of the incident. |[ ]
|  |  | If the Incident Management Team is assembled, it will designate an Incident Controller, who will be the point of contact for the incident, until recovery is complete. The IMT will communicate with the Board to keep them updated.  |[ ]
|  |  | If life and or safety are at immediate risk, the Incident Controller and his team shall first act to ensure their own safety as well as those around them and look to communicate as soon as the situation allows. |[ ]
|  |  | If necessary, the Board will designate a Communications representative to liaise with the press / media. The Communications representative will be kept updated with ‘need to know’ information by the Incident Controller. |[ ]
|  |  | The Incident Controller will ascertain the situation and will decide if the situation requires escalation, based on reports received and investigations carried out locally. In the event that the incident could impact on technology availability, the ICT Department will also be notified. Assuming escalation, the Incident Controller will liaise with a member of staff authorised to invoke the Business Continuity Recovery Procedures defined within this document.  |[ ]
|  |  | If a disaster situation **IS NOT** declared, then the incident is dealt with locally and resolved. The Incident Controller updates the Board accordingly. |[ ]
|  |  | If a disaster situation **IS** declared, the Incident Controller will liaise with a member of staff authorised to invoke the Business Continuity Recovery Procedures and will launch emergency response procedures defined within this document. |[ ]
|  |  | The Incident Controller will keep the Communications Representative updated as to the status of the event. |[ ]
|  |  | The Incident Controller will notify all staff of the incident and of operational status |[ ]
|  |  | The incident management and business continuity plans continue until the incident has been resolved. |[ ]

|  |  |  |
| --- | --- | --- |
|  | 7.2 | 2BIncident Management Team StructureA successful recovery from a disaster can only occur with total coordination of all incident management and recovery activities. In a crisis, each team has specific functions that contribute to the success of the recovery. The following diagram shows the structure of an Incident Management Team (IMT), particularly in the aftermath of an incident.  |
|  |  |  |
|  |  | 27B7.2.1 Incident Management Team |
|  |  | The Incident Management Team (IMT) assess the physical and operational status of the business location immediately following an incident; determines the need for personnel evacuations; reviews the situation with security and management as needed; reviews the situation with emergency services (Fire, Police, Ambulance as necessary); provides input to the process for declaring a crisis or emergency as needed and generally coordinates the planning and operational aspects of the incident. The (IMT) also makes and effort to reduce and control the impact of the incident on the location. |
|  |  |  |

|  |
| --- |
| 8.0 Notification, Escalation and Declaration |
|  |  |  |
|  | 8.1 | 3BIntroduction |
|  |  | During any interruption, personal safety is the primary concern. Managers should periodically review emergency response and evacuation procedures with their staff to ensure familiarity with safety procedures.Employees should notify their manager of any operational disruption or emergency situation. In the event of an emergency, project managers are authorised to declare a disaster on behalf of the local project ONLY.The notification plan is designed for use in mobilising an Incident Management Team. If partial mobilisation is needed, the appropriate portion of the plan can be executed accordingly. When Primary IMT members cannot be reached for their part in the notification plan, their alternates will be contacted. |
|  | 8.2 | 4BNotification Process Overview |
|  |  | 28B8.2.1 Initial NotificationDuring normal business hours, contact personnel at the following numbers:*Divisional Director:***(SECTION REDACTED)***Operations Director / Senior Manager***(SECTION REDACTED)** |
|  | 8.3 | 5BNotification Process (Emergencies ONLY)Communication during a crisis is CRITICAL. As such, follow local notification protocols in an emergency.In the event of a crisis, the following table will be populated and distributed to all Incident Management Team members |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Contact Number | Home Number | Location |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

 |
|  |  |  |
|  | 8.4 | 6BIncident Response Assembly Locations |
|  |  | 29B8.4.1 Erith House Assembly LocationGarages adjacent to Front Car Park |
|  |  | 30B8.4.2 Anchor Bay Wharf Assembly LocationTipper Drivers’ car park (100m directly opposite from gate) |
|  |  |  |
|  | 8.5 | 7BEscalation Process (Emergencies ONLY) |
|  |  | **Step 1:** Follow local established emergency escalation and life/safety protocols. If these are not available, the first employee to become aware of an incident should immediately report it to local management, who will escalate the information to the Incident Management Team Leader or his/her designated alternate. |
|  |  | **Step 2:** Continue to follow local established emergency escalation and life/safety protocols. If these are not available, based on the results of local, regional discussions a decision will be made on declaring a disaster: * 1. IF a disaster IS NOT declared, the Incident Manager will coordinate with other local management and Group staff to restore normal business operations accordingly.
	2. IF a disaster IS declared, the Incident Manager, the Board of Directors, will invoke the Business Continuity plan.
 |
|  | 8.6 | 8BPlan Authorisation and Declaration |
|  |  | When the Incident Management Team is notified of the event, they will contact the local business leadership on the incident, asking them to remain on standby. The IMT will report to the scene of the event, or where directed, and coordinate additional activities. Making Directors and Senior management aware begins after authorisation has been given to declare a disaster. |
|  | 8.7 | 9BDeclaration Process (Emergencies ONLY)The disaster declaration process is as follows: |
|  |  | 1. Only the management team in charge of each individual division or Business or his/her appointed person has the authority to declare a disaster.
2. A disaster declaration MUST generally meet one of more of the following criteria:
	1. The incident is a major, prolonged or indefinite disruption to business as usual.
	2. The incident is of sufficient magnitude (casualties/fatalities/property and or facility damages/business disruptions, etc) and warrants the enactment of emergency response and incident management measures to ensure continuity of operations)
	3. The incident has met and / or exceeded the threshold of disaster declaration criteria for appropriate major public sector entities on a local, regional, national or international level.
	4. Not declaring the incident a ‘disaster’ poses a direct threat to the viability of any of the Erith Group companies as a business.
 |
|  |  |  |
|  |  |  |

# 9.0 Incident Response Checklists

## 9.1 Key Personnel Contact Lists

(To be completed when the Business Continuity Plan is invoked)

|  |
| --- |
| **Incident Management Team** |
| Name | Role | Mobile | Landline | Alternate Phone |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| **Logistics Team** |
| Name | Role | Mobile | Landline | Alternate Phone |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| **Planning Team** |
| Name | Role | Mobile | Landline | Alternate Phone |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| **Finance and Administration Team** |
| Name | Role | Mobile | Landline | Alternate Phone |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 9.2 Key Suppliers (Purchasing) – Erith Group

**(SECTION REDACTED)**

## 9.4 Key Suppliers (ICT)

**(SECTION REDACTED)**

## 9.5 Utilities and Regulators

**(SECTION REDACTED)**

|  |  |  |
| --- | --- | --- |
|  | 9.6 | 10BKey Suppliers (Bankers) |
|  |  | **(SECTION REDACTED)** |
|  | 9.7 | 11BPasswords**(SECTION REDACTED)** |
|  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 10.0 Team Responsibilities |
|  | 10.1 | 12BInitial Incident Management Team Meeting |  |
|  |  | Ensure that an initial exploratory meeting has been set. The details should be forwarded to all members of the team and their presence should be recorded using the RECOVERY TEAMS PERSONNEL ASSIGNMENT FORM found in the Recovery Forms section of this document. |[ ]
|  |  | Ensure that any missing IMT members, their alternates and any additional personnel are notified of the meeting. See the KEY CONTACTS section of this guide for a complete list of IMT members and alternates, and their contact information. |[ ]
|  |  | Obtain a current situation report. Address the following key issues:1. Type of event (fire, weather, terrorism, power outage, telecomm outage, etc.)
2. Specific location of event, if known (building, floor, side of floor, etc.)
3. Magnitude of the event
4. Time of event
5. Suspected cause
6. Emergency/evacuation procedures status
7. Emergency Services notified, and when.
8. Injuries or fatalities
9. Building access status (current access, near-term potential access)
10. Immediate impact to business operations
11. Potential for news media attention
 |[ ]
|  |  | Ensure that a member of the IMT documents, in chronological order, incident milestones and actions taken using the BUSINESS INTERRUPTION REPORT template in the Recovery Forms section of this policy. This form will be used as a tool to update the IMT and other senior management. |[ ]
|  |  | If required, provide advice to local senior management whether employees should be sent home. Local senior management will develop a statement, determine method of communicating updates and communicate to employees. |[ ]
|  |  | Follow up to ensure that local management has decided whether or not to intercept phone lines with a customised emergency voice recording or redirect incoming calls as necessary |[ ]

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | 10.2 | 13BIncident Management Team Checklist |  |
|  |  | Gather information about the incident from first-hand contact, available first responders, employees, and others; relays to Incident Manager.  |[ ]
|  |  | Account for all staff/guests on (and if applicable off) premises. |[ ]
|  |  | Administer first aid and/or ensures life/safety measures as appropriate. |[ ]
|  |  | Inform building security and the landlord if they are not already aware of the incident. Landlord’s details within key suppliers section. |[ ]
|  |  | Conduct an initial assessment of the incident’s likely impact on local operations. |[ ]
|  |  | Distribute information to local employees on the incident. |[ ]
|  |  | Provide information about the incident to first responder organisations. |[ ]
|  |  | Establish and maintain communications with the appropriate business unit. |[ ]
|  |  | Provide input as directed to the disaster declaration process. |[ ]
|  |  | If disaster is declared, support the Incident Management plan response. |[ ]
|  |  | If a disaster is not declared, support recovery from the incident and restore operations accordingly. |[ ]
|  |  | Provide ongoing review and analysis of incident(s) with distribution of information to staff. |[ ]
|  |  | Coordinate with Operations Section leadership as well as third-party organisations to ensure that required resources are in place and ready for delivery to affected venue. |[ ]
|  |  | Support Communications Representative and Safety Officer roles. |[ ]
|  |  | Support management of the incident and restores operations accordingly. |[ ]
|  |  | Support post-event demobilisation plan as needed.  |[ ]
|  |  | Assist IMT and Incident Manager as directed. |[ ]
|  |  | Provide post-event report of activities. |[ ]

|  |  |  |  |
| --- | --- | --- | --- |
|  | 10.3 | 14BIncident Manager Task ChecklistThe following recommended sequence of actions should be provided by the local incident team leader and/or incident manager after completing the Initial Response checklist in Section 7.1  |  |
|  |  | Assumes overall leadership of all incident management activities.  |[ ]
|  |  | Receives information about the incident from IMT, first responders, employees, and others.  |[ ]
|  |  | Delegates the accounting for of all staff/guests on (and if applicable off) premises. |[ ]
|  |  | Ensures that first aid is being provided; ensure that life/safety measures are being delivered. |[ ]
|  |  | Updates the Board with information as soon as practical. |[ ]
|  |  | Assesses the incident’s likely impact on local operations.  |[ ]
|  |  | If assessment of the incident suggests a serious event that could adversely impact operations. |[ ]
|  |  | Provides input as directed to the disaster declaration process. |[ ]
|  |  | Based on input from all sources determines if/when to declare a disaster. |[ ]
|  |  | If a disaster is declared, facilitates activation of IM plan; informs others. |[ ]
|  |  | If a disaster is not declared, manages recovery from the incident and restore operations accordingly. |[ ]
|  |  | Leads the launch of Communications Rep and Safety Officer Roles |[ ]
|  |  | Manages the incident and restores operations accordingly. |[ ]
|  |  |  |  |
|  | 10.4 | 15BIncident Response Recommended Actions |  |
|  |  | The Incident Manager will develop recommendations for senior management on what overall response strategies should be implemented to facilitate the recovery of business operations in the most timely, efficient and cost-effective manner. |[ ]
|  |  | Consider information gathered in earlier incident and damage assessments including, but not limited to, the following:The area(s) affected by the disaster;Anticipated duration of incident;Availability of required employees;Any special timing issues such as relation­ship to month-end, quarter-end, etc.;Any special business issues (e.g., unusual business volume or backlog, unusual contractual obligations);Regulatory obligations;Salvageable equipment and supplies Availability of equipment and supplies at potential alternate or off-site locations;Salvageable records required for recovery activities; andRecords which require intensive reconstruction activities. |[ ]
|  |  | Develop critical business function recovery priority lists for the following periods:8 hours12 hours24 hours72 hours or longer |[ ]
|  |  | Recommend to the Board where critical business functions and IT operations can be recovered based upon the following priority: * Return to building
* Local sites
* Other sites
 |[ ]
|  |  |  |  |
|  | 10.5 | 16BActions following a disaster declaration |  |
|  |  | Based on observations from local management, senior management or the emergency services, the Incident Manager will launch an incident management plan that facilitates a safe and rapid evacuation of staff. |[ ]
|  |  | If not already identified locally, Incident Manager should identify and communicate the recommended assembly site(s) to local IMT members, local management, and the Business Recovery Team. |[ ]
|  |  | Ensure that the local IMT convenes a meeting to review response and recovery options.  |[ ]
|  |  | Distribute the current situation to all team members. General points to be covered include the following:1. Type of event (fire, weather, terrorism, power outage, telecomm outage, etc.)
2. Specific location of event, if known (building, floor, side of floor, etc.)
3. Magnitude of the event
4. Time of event
5. Suspected cause
6. Emergency/evacuation procedures status
7. Emergency Services notified
8. Injuries and fatalities
9. Building access (current access, near-term potential access)
10. Immediate impact to business operations
11. Potential for media (e.g., television, radio) attention
 |[ ]
|  |  | Assign an IMT member responsibility to document, in chronological order, incident milestones and actions taken using the BUSINESS INTERRUPTION REPORT template in the Recovery Forms section of this policy. This form will be used as a tool to update senior management. |[ ]
|  |  | The Incident Manager will decide whether to intercept phone lines with a customised emergency voice recording.Main Message in the first 24 hours:*“Welcome to the Erith Group. We’re sorry, but our normal business operations have been interrupted due to XXXXX. Please be patient as we are making every effort to recover operations as soon as possible. We expect to resume normal service on or about XXXX.”*  |[ ]
|  |  | Assist with acquisition of resources as needed |[ ]
|  |  | Provide regular updates to Communications Rep and other points of contacts. |[ ]
|  | 10.6 | 17BCommunications Officer Task Checklist |  |
|  |  | When activated, establishes communications with organisations as indicated in incident management plan. |[ ]
|  |  | Establish regular time frames for reporting incident and recovery status to designated organisations. |[ ]
|  |  | Process incoming messages from and external organisations, including police/fire and the media. |[ ]
|  |  | Distribute approved messages to designated parties when directed. |[ ]
|  |  | Assists IMT and Incident Manager as directed. |[ ]
|  |  | Provide post-event report of activities. |[ ]
|  |  |  |  |
|  | 10.7 | 18BSafety Officer Task Check List |  |
|  |  | When activated, monitors and manages physical safety conditions.  |[ ]
|  |  | Develop measures to ensure safety of personnel. |[ ]
|  |  | Assist in the administering of first aid and/or ensure life/safety measures as needed. |[ ]
|  |  | Assist Incident Manager as directed.  |[ ]
|  |  | Provide post-event report of activities.  |[ ]
|  |  |  |  |
|  | 10.8 | 19BPlanning Team Task Checklist |  |
|  |  | When activated, prepare Incident Action Plan.  |[ ]
|  |  | Maintain situation and resource status. |[ ]
|  |  | Coordinate the preparation and distribution of incident documentation. |[ ]
|  |  | Provide location for subject matter and technical expertise.  |[ ]
|  |  | Prepare demobilisation plan as needed.  |[ ]
|  |  | Assist Incident Manager as directed. |[ ]
|  |  | Distribute information and messages to appropriate departments and individuals. |[ ]
|  |  | Provide post-event report of activities. |[ ]
|  |  |  |  |
|  | 10.9 | 20BFinance and Administration Task Checklist |  |
|  |  | When activated, facilitate various administration and financial activities. |[ ]
|  |  | Monitor incident costs and maintains financial records. |[ ]
|  |  | Address insurance and workmen’s compensation issues. |[ ]
|  |  | Facilitate procurement activities, e.g., contracts. |[ ]
|  |  | Monitor timekeeping and related activities. |[ ]
|  |  | Disseminate information and messages to appropriate departments and individuals. |[ ]
|  |  | Assist Incident Manager as directed. |[ ]
|  |  | Provide post-event report of activities. |[ ]
|  |  |  |  |
|  | 10.10 | 21BPre Incident Preparation |  |
|  |  | Establish divisional response plans and procedures for dealing with incidents. |[ ]
|  |  | Establish communications process for distributing information about an incident to the Incident Management Team. |[ ]
|  |  | Point of contact for compiling information on incidents and reporting to senior management. |[ ]
|  |  | Train alternate(s) assigned as backup to Incident Manager. It is entirely possible that an Incident Manager would be found from any divisional personnel |[ ]
|  |  |  |  |
|  | 10.11 | 22BActions following an incident and prior to disaster declaration |
|  |  | Gather input from the local personnel and local senior management.  |[ ]
|  |  | Analyse the input and complete an initial assessment of the situation. Attempt to determine the potential for an evacuation or other activity that would negatively impact operations at the site. |[ ]
|  |  | Forward the assessment results and any other intelligence to the Incident Manager for analysis and action.  |[ ]
|  |  | Coordinate incident analysis with local personnel. |[ ]
|  |  |  |  |
|  | 10.12 | 23BActions during and after the disaster |  |
|  |  | Follow up to ensure that Divisional leaders have notified their respective recovery team members. Document notifications in the PERSONNEL NOTIFICATION CONTROL LOG found in the Recovery Forms section of this guide. |[ ]
|  |  | Notify any other corporate contacts and third parties as deemed necessary. See the KEY CONTACTS section of this guide for contact information. |[ ]
|  |  | Follow up to ensure that information regarding the status of the incident and the company’s response to it is regularly communicated to the appropriate individuals and organisations. |[ ]
|  |  | Be available to answer questions and provide input to other organizations as they enter the incident response/recovery process |[ ]
|  |  | Be available to answer questions and provide input to other organizations as they enter the post-incident recovery and evaluation process.  |[ ]

Signed for and on behalf of

The Erith Group



Steven Darsey

Chairman

1. **WAN** – Wide Area Network [↑](#footnote-ref-2)
2. **MPLS** – Multiprotocol Label Switching is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows. [↑](#footnote-ref-3)
3. **IPSec** - Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks. [↑](#footnote-ref-4)
4. **SDWAN** is an acronym for software-defined networking in a wide area network. SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism [↑](#footnote-ref-5)