

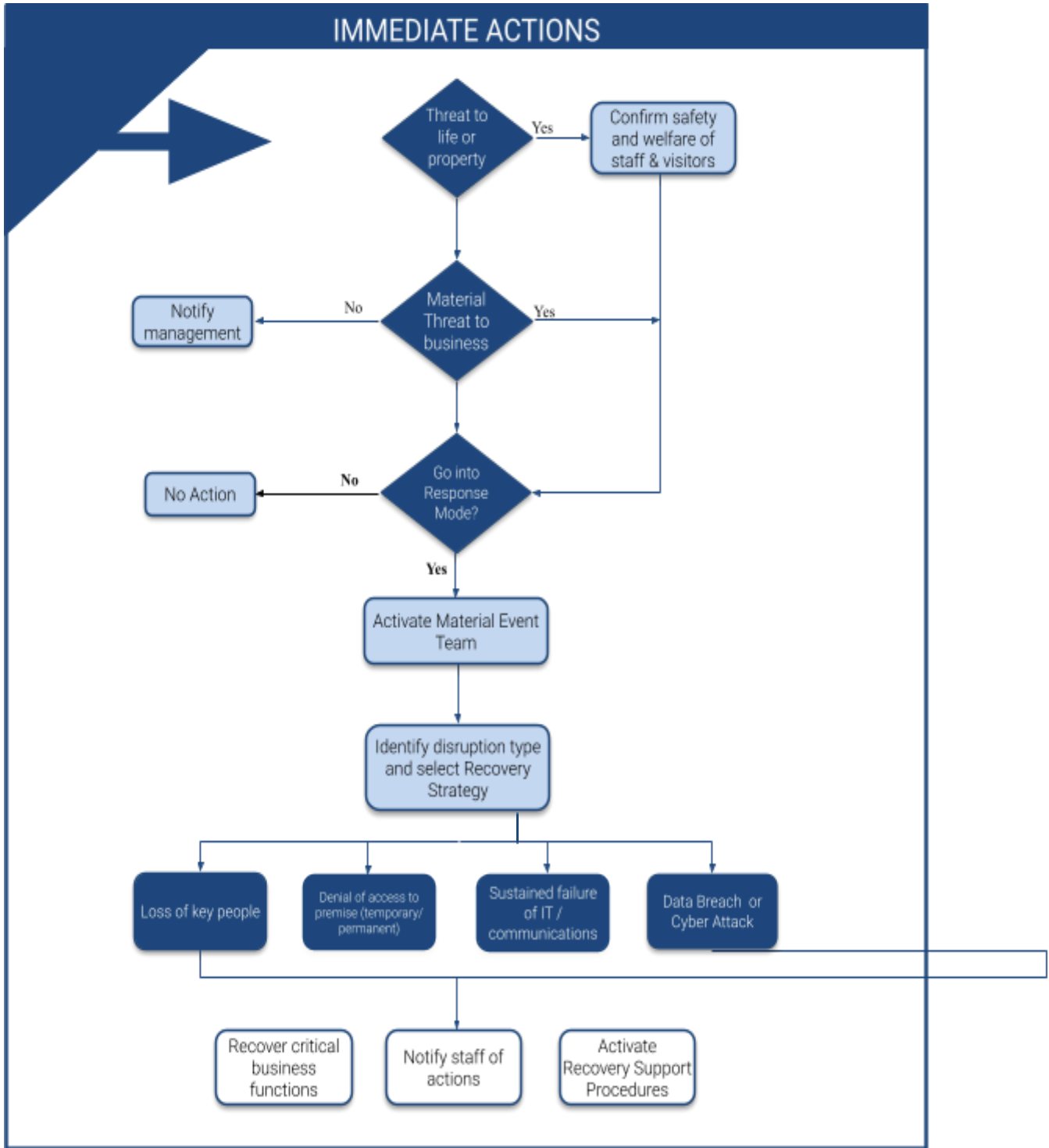
Material Event Plan

BITS Technology Group

Introduction & Overview

This Material Event Plan (MEP) is to be used to restore BITS Technology Group’s business operations in the event of a major incident or other business interruption event. This process and reference to supporting tools is described below:

Business Recovery Process



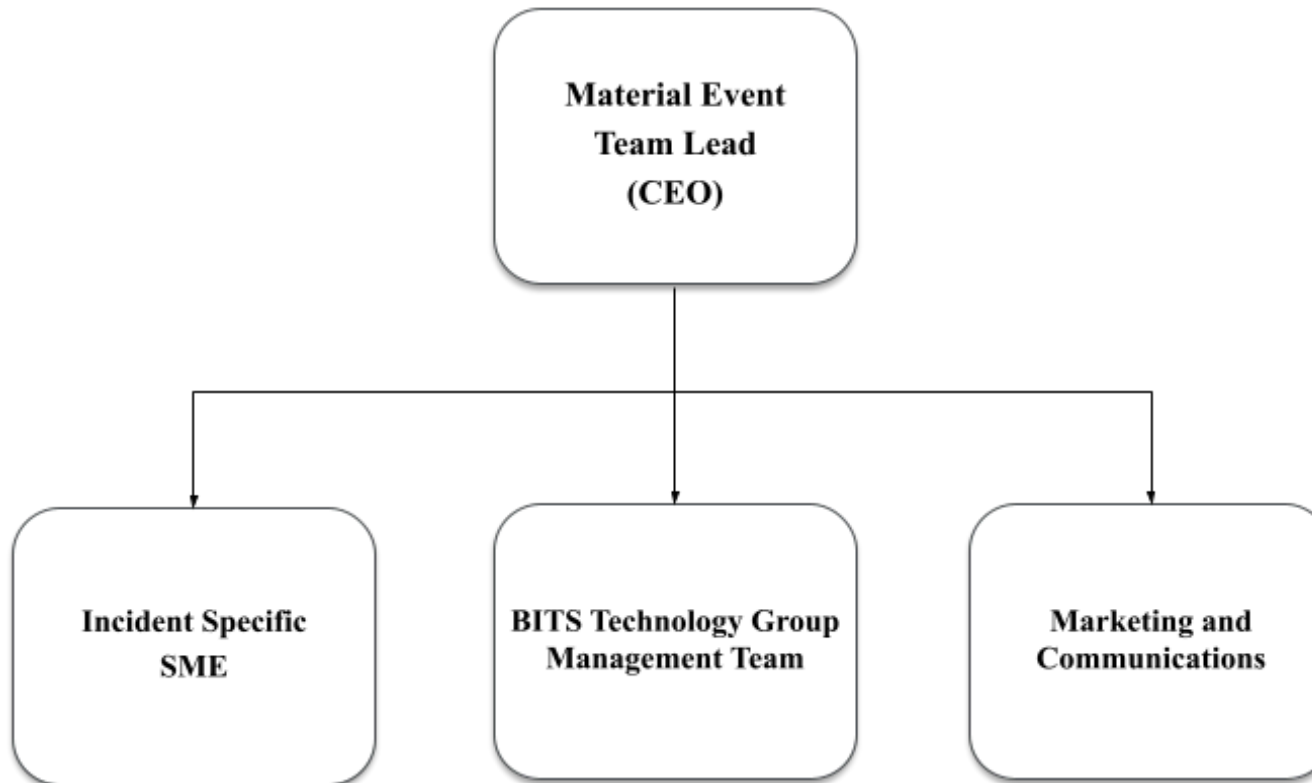
Phase 1 Manage the Disruption

Activate Material Event Team

Activate Command Centre

1.1 Activate Material Event Team

The BITS Technology Group *Material Event Team* (MET) as outlined below will be responsible for the operational management of an incident including response and recovery. The Material Event Team will liaise with other stakeholders as required to ensure appropriate management of major incidents.



1.2 Activate Command Centre

The following Command locations have been identified for the Material Event Team to coordinate business recovery operations from in the event of a major incident.

Primary Site	
BITS Technology Group Head office 4 Watts Drive Varsity Lakes QLD 4227	
Activation procedure	
1.	Confirm availability of dedicated Command Centre.
2.	Create Dial-in bridge for remote participants using Zoom

In the event the primary site is not available, a virtual command centre will be established using Microsoft Teams Calling.

Secondary Site	
Note If the 'Microsoft Teams Calling' platform is assumed unavailable during Cyber or IT related outage, the MET Lead will communicate an alternate platform such as Discord or Zoom.	
Activation procedure:	
1.	Notify all participants of virtual command centre
2.	Create Dial-in bridge for remote participants using Microsoft Teams Calling

Phase 2: Recover Critical Functions & Resume Business Operations

2.1 Initial Meeting Agenda

2.2 Critical Business Functions

2.3 Business Impact Assessment

2.4 Select Recovery Strategy

2.5 Ongoing Meeting Agenda

2.1 Initial Meeting Agenda

No.	Agenda Item	By whom	✓
1	Convene meeting and confirm welfare of all MET Members.	MET Lead	<input type="checkbox"/>
2	Confirm MET roles & responsibilities.	MET Lead	<input type="checkbox"/>
3	Identify impacted Critical Business Functions (Section 2.2)	All MET members	<input type="checkbox"/>
4	Assess any additional business impacts because of the disruption and allocate immediate tasks to members of the MET.	All MET members	<input type="checkbox"/>
5	Based on the incident and the impact assessment, select appropriate Recovery Strategy, and allocate those tasks.	All MET members	<input type="checkbox"/>
6	Confirm 'Problem Ownership' (i.e. what part of this problem does BITS Technology Group Own, and what part can it influence?)	All MET members	<input type="checkbox"/>
7	Agree protocols for initial communications – audience, frequency, format, and content (Appendix 5).	MET Lead	<input type="checkbox"/>
8	Agree time of follow-up meeting to provide update on actions and outcomes.	MET Lead	<input type="checkbox"/>
9	Close meeting.	MET Lead	<input type="checkbox"/>

2.2 Critical Business Functions

Task or Process	Business Unit	MAO*	RTO**
Monitor Infrastructure and Security	BITS Technology Group	24 hours	12 hours
Provide customer service and service delivery support to customers via phone and email.	BITS Technology Group	12 hours	12 hours
Provide escalation support for complex infrastructure faults.	BITS Technology Group	72 Hours	72 Hours
Provide legal advice/manage regulatory and compliance obligations	BITS Technology Group	72 Hours	72 Hours
Manage sales enquiries (all divisions)	BITS Technology Group	12 Hours	12 Hours
Coordinate and manage payroll and reporting obligations	BITS Technology Group	72 Hours	72 Hours
Ongoing maintenance of infrastructure and identifying infrastructure related issues: - Updating software versions - Fixing Bugs - Remediating Vulnerabilities	BITS Technology Group	7 Days	24 hours
Oversee business performance reporting and advisory.	BITS Technology Group	24 Hours	24 Hours
Oversee Human Resources: - Recruitment - Employee police checks - Learning and Development - General Staff Engagement	BITS Technology Group	72 Hours	72 Hours

* Maximum Acceptable Outage

** Recovery Time Objective

2.3 Business Impact Assessment

Use the following Impact Assessment tool to forecast strategic impacts to BITS Technology Group resulting from the incident.

Health, Safety and People	
To what extent is the event likely to impact the health and safety of BITS Technology Group employees, visitors and contractors?	
Impact and Secondary effects	
Mitigating Actions	Ownership

Regulatory/Compliance/Governance	
To what extent is the event likely to result in an impact to BITS Technology Group Regulatory, Compliance or Governance standing?	
Impact and Secondary effects	
Mitigating Actions	Ownership

Reputation/Community or Strategic	
To what extent is the event likely to result in a strategic impact or reputational damage to BITS Technology Group?	
Impact and Secondary effects	
Mitigating Actions	Ownership

Customer Experience	
To what extent is the event likely to result in a loss of customers or an impact of customer experience?	
Impact and Secondary effects	
Mitigating Actions	Ownership

Business Operations	
To what extent is the event likely to result in an impact on internal BITS Technology Group operations?	
Impact and Secondary effects	
Mitigating Actions	Ownership

Information Security	
To what extent is the event likely to impact BITS Technology Group Information Security?	
Impact and Secondary effects	
Mitigating Actions	Ownership
Most Likely Scenario	
What is the most likely outcome of the situation? What further actions need to be taken to address these impacts?	
Impact and Secondary effects	
Mitigating Actions	Ownership
Worst Case Scenario	
What is the worst-case outcome of the situation? What further actions need to be taken to prevent this scenario?	
Impact and Secondary effects	
Mitigating Actions	Ownership

2.4 Select Recovery Strategy

Based on the type of disruption that occurred and the impacts assessed, select the appropriate Recovery Strategy. The Business Recovery Coordinator should then oversee implementation of this strategy with affected Business Units.

Type of Incident	Recovery Strategies
<ul style="list-style-type: none"> ▪ Industrial action ▪ Resignation of key employees ▪ Illness or injury ▪ Kidnap ▪ Disease outbreak 	<p>1. Loss of Key People/Employees</p>
<ul style="list-style-type: none"> ▪ Minor structure fire or smoke damage ▪ Electrical failure ▪ Water damage ▪ Receipt of suspicious mail ▪ Security/access malfunction ▪ Civil disturbance ▪ Armed hold-up ▪ Physical disaster ▪ Major structure fire ▪ Other physical disaster ▪ Terrorism incident 	<p>2. Denial of Access to Premises (Temporary/Permanent)</p>
<ul style="list-style-type: none"> ▪ Software or hardware failure ▪ Successful Malicious Attack ▪ IT systems failure ▪ IT communications failure ▪ Theft, fraud or malice ▪ Human error or negligence 	<p>3. Sustained Loss of IT and/or Communications Systems</p>
<ul style="list-style-type: none"> ▪ Release of secure or confidential information to an untrusted environment ▪ Denial-of-service (DoS) and distributed denial-of-service (DDoS) ▪ Phishing attack ▪ Malware attack 	<p>5. Data Breach / Cyber Attack</p>

+

Continue on with the actions provided in the selected Recovery Strategy below.

This Recovery Strategy will provide a step-by-step guide for recovering your critical business functions.

Follow steps below in the selected Recovery Strategy to recover critical business functions.

Recovery Strategy # 1		Loss of Key People/Employees		
Step	Timing	Responsibility	Activity/Action/Task	Reference
1.	0-2 hrs	MET	Assemble remaining employees and contractors at the office, site or virtual assembly area.	-
2.	0-2 hrs	MET	Assess wellbeing of employees and/or contractors. Brief employees regarding the incident if appropriate.	-
2.	0-2 hrs	MET	If premises are accessible and deemed safe, employees should re-enter.	-
3.	0-2 hrs	MET	If the site is unusable or unsafe, activate 'Denial of Access to Premises' Recovery Strategy.	Section 2.4
4.	2-4 hrs	MET	Assess all work-in-progress affected by loss of employee/s.	-
5.	2-4 hrs	MET	Identify internal alternate employees or contractors to carry out Critical Business Functions.	Section 2.2
6.	2-4 hrs	MET	In the case of serious injury or death, develop appropriate communications strategies.	
7.	4-12 hrs	MET	Employees/contractors to resume business operations in accordance with critical business functions list.	Section 2.2
8.	12-24 hrs	MET	Confirm that impacted employees have access to on-going trauma counselling services, if required.	
9.	Daily	MET	Provide a regular status report to Directors on critical business capabilities.	-
10.	1 week +	MET	Commence recruitment of permanent employees to replace key roles as needed.	-
11.	Continue with Post Incident Actions			Section 3.1

Recovery Strategy # 2		Denial of Access to Premises (Temporary/ Permanent)		
Step	Timing	Responsibility	Activity/Action/Task	Reference
1.	0-2 hrs	MET	Determine likely downtime estimates.	-
2.	0-2 hrs	MET	Inform all staff to work remotely.	

Recovery Strategy # 3		Sustained Failure of IT and/or Communications Systems		
Step	Timing	Responsibility	Activity/Action/Task	Reference
1.	0-2 hrs	MET	Confirm if the Information Security controls in place are negatively impacted.	
2.	2-4 hrs	MET	If telephone communications are affected, divert phones.	
3.	2-4 hrs	MET	If an extended downtime is anticipated (> 24 hours), liaise with IT to determine the requirement to activate 'Denial of Access to Premises' Recovery Strategy.	Section 2.4
4.	6-12 hrs	MET	If disruption extends to customers, develop communications strategy to notify of disruption, likely downtime and changes to services.	
5.	6-12 hrs	MET	Review critical business functions list to assess all functions that might be impacted.	Section 2.2
6.	6-12 hrs	MET	Procure replacement IT equipment/alternate service provider as determined by disruption assessment.	
7.	6-12 hrs	MET	Establish a Recovery Plan for any disrupted critical business functions including: <ul style="list-style-type: none"> - Implementation of redundancies and work-around - Requirement for relocation of employees - Incident communications to affected parties - Management of other business impacts caused by the failure of IT services 	-
8.	Continue with Post Incident Actions			Section 3

Recovery Strategy # 4		Data Breach / Cyber Attack		
Step	Timing	Responsibility	Activity/Action/Task	Reference
1.	0-2 hrs	MET	Determine extent of impacted systems and anticipated downtime (if any).	
2.	0-2 hrs	MET	Confirm if the Information Security controls in place are negatively impacted.	
3.	0-4 hrs	MET	Provide update to MET on identification and assessment actions.	
4.	2-4 hrs	MET	Determine requirement to involve external forensic experts before attempting containment or response actions.	
5.	2-4 hrs	MET	Confirm impacted Critical Business Functions and review any manual workarounds if required.	Section 2.2

Recovery Strategy # 4		Data Breach / Cyber Attack		
5.	2-4 hrs	MET	Liaise with IT on a regular basis to keep abreast of the situation and expected recovery timeframes.	
1.	6-12 hrs	MET	Develop internal and external communications strategies to notify key stakeholders of the incident.	
2	6-12 hrs	MET	If customer data has been breached, determine legal implications, regulatory reporting requirements and member communications.	-
3.	6-12 hrs	MET	Determine reporting requirements to the Australian Cyber Security Centre.	-
4.	6-12 hrs	MET	Develop ongoing internal and external communication strategies to update key impacted stakeholders.	
5.	Daily	MET	Provide a daily status report to Directors on recovery capabilities.	
6.	Continue with Post Incident Actions.			Section 3

Phase 3: Post Incident Actions

Conduct Post Incident Review

Points to cover during a PIR:

Element	Description
Emergency Response	<ul style="list-style-type: none"> ● Was an evacuation required? ● Were any employees injured or affected by the incident? ● Was the building secured to prevent re-entry? ● Were evacuation details reported to the Material Event Team?
Business Impacts	<ul style="list-style-type: none"> ● Was the MET Lead or a Material Event Team member notified of the disruption / incident in a prompt manner? ● Was a Material Event Team member easily reachable? ● Was a business impact assessment conducted? How was this information used? ● Were the premises affected and deemed unusable? ● Were critical business functions likely to be affected? ● Was the Information Security of BITS Technology Group negatively impacted during the event? ● Was the MEP activated? If yes, was a response strategy followed and if so which?
Recovery	<ul style="list-style-type: none"> ● Were recovery strategy tasks reviewed on a regular basis? ● Were critical business functions restored within agreed timeframes? If not, why not and which functions were affected? ● Were customers affected? ● Was activation of alternate sites required? If so, were they fully operational within agreed timeframes?
Communication	<ul style="list-style-type: none"> ● Were all key stakeholders notified? ● Was stakeholder communications appropriate? ● Was stakeholder communications timely? ● Was the media communicated with? ● Was media communication appropriate? ● Were the communication templates used? ● Was an action log maintained throughout?
Resumption	<ul style="list-style-type: none"> ● Were ongoing site security issues addressed? ● Were long term restoration/relocation strategies assessed?

Appendices

4. Stakeholder Contact Details

A4: Stakeholder Contact Details

Material Event Team

Material Event Team Position	Name	Job Title	Mobile Phone
MET Lead	Bernard Mangelsdorf	CEO & Head of Sales and Marketing	0438129766
Management Team	Blair Munro	Head of Technology	0400499644
	Jesse Whitton	Head of Service	0422380933
	Esther Mangelsdorf	Head of Finance and HR	0478146000

* Note: If the CEO is unavailable, Head of Technology will become the MET Lead.

Document Control

DESIGNATED POLICY OWNER	Classification	Publication Date	Next Review Date
CEO	Business Confidential	14/5/2025	14/5/2026

Revision History

Version	Date	By	Summary of Changes
0.1	28/4/2025	Esther Mangelsdorf	Initial draft
1.0	14/5/2025	Esther Mangelsdorf	Published Copy
1.1	04/06/205	Esther Mangelsdorf	Updated Material Event team details. Changed command centre from Google Meet to Discord as per feedback from training exercise. Published Copy