©(ORGANISATION NAME)

INCIDENT MANAGEMENT POLICY

Subject: Incident Management Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 24	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

This document is the property of CcHUB. Circulation is restricted to the Organisation’s use. It must not be copied or used for any other purpose other than for which it is supplied, without the expressed written authority of CcHUB.

Except where provided for purposes of contractual requirements, CcHUB disclaims any responsibility or liability for any use or misuse of the document by any person and makes no warranty as to the accuracy or suitability of the information to any third party. Any misuse of the document is addressable by CcHUB.

CONTENTS

1.0 INTRODUCTION

Incidents are disruptions to normal operations of an Organisation. Security incidents do not necessarily disrupt the normal operations of an Organisation but can compromise the data/information and information processing facilities of the Organisation.

Reference	Description of Risk
SAFETag	Incident Response and Emergency
SAFETag	Suspicious Activity Monitoring and Analysis
SAFETag	Digital Forensics and Evidence Capture

1.1 PURPOSE

The Organisation has a responsibility to monitor all incidents that occur within the Organisation that may impact on the confidentiality, integrity, availability, or accountability of information. All incidents need to be identified, reported, investigated, and monitored. This Policy defines the requirements to ensure information security management incidents are reported and managed effectively within the Organisation.

The aim of incident management is to prevent or minimise harm or detriment to customers or employees. Others include:

- To define appropriate mechanisms for responding to information security incidents.
- To ensure that information asset owners are appropriately identified and are informed of security incidents.
- To assign responsibilities for the information security incident response management process.
- To ascertain the seriousness and impact of an incident.
- To identify any vulnerability created by an information security incident.
- To estimate the resources that are required to mitigate the incident.
- To ensure that proper post-incident reporting occurs and that procedures are reviewed and adjusted to mitigate risk and prevent future incidents.

1.2 OBJECTIVES

The objective of this policy is to ensure that incidents are:

- Effective maintenance of the confidentiality, integrity, and availability of information resources within the Organisation through timely identification and handling of incidents
- Incidents are promptly identified and reported.
- Incidents are adequately logged and tracked for remediation.
- Incidents are efficiently resolved in a timely manner.

1.3 CLASSIFICATION OF INCIDENTS

Classification	Severity	Description	Timeline
Critical Incidents	4	Incidents of the highest severity level pose a severe and immediate threat to business operations, data integrity, or customer safety. Critical incidents demand immediate attention and an escalated response to minimise potential damages and restore normal operations quickly. For example, cybersecurity breaches, natural disasters, ransomware attacks, etc.	xx Hours
High Incidents	3	Incidents with a significant impact on business operations or data, though not as critical as the highest severity level. High incidents require prompt response and resolution to prevent further escalation and mitigate potential consequences on productivity and customer trust. For example, server outages, supply chain disruptions, employee health incidents, etc.	xx Hours
Medium Incidents	2	Incidents with moderate impact may cause disruptions, but their consequences are more manageable, allowing Organisations to respond effectively without immediate escalation. Nevertheless, timely resolution remains essential. For example, network slowdown, data entry errors, and local power outages.	xx Hours
Low Incidents	1	Incidents with minimal impact on business operations, often involve isolated issues or minor disruptions that do not pose a significant threat. Low incidents require attention, but they can be resolved without immediate urgency, allowing Organisations to address them within standard response timeframes. For example, printer malfunction, minor equipment damages, or temporary network glitch.	xx Hours

1.4 POLICY STATEMENTS

1.4.1 All types of incidents shall be defined and categorised in terms of their severity. This definition and categorisation of incidents shall assist in assessing the associated risk to the business and the urgency with which the incident shall be responded to.

1.4.2 All incidents with a severity of 2 or higher (refer to section 1.2) shall be recorded; Evidence (for incidents) shall be gathered within the stipulated response time to ensure that the incident is adequately addressed.

1.4.3 Impacted stakeholders (internal users, third-party client(s), contractors, etc.) shall be made aware of what constitutes an incident and how to react to incidents; Users of information resources shall be made aware of the different types of incidents and the associated Incident Management Procedures. They shall be required to note and report any observed or suspected security weaknesses in or threats to systems or resources. Incidents shall be reported to the IT Service Desk using the Request Management Portal.

1.4.4 Internal users, third-party client(s), and contractors shall not attempt to test or identify any suspected weakness, as testing/analysing weaknesses shall be interpreted as a potential misuse of the system.

1.4.5 The Organisation shall establish a formal incident response plan. The plan shall be backed up by an incident management procedure that shall document what actions to be taken in the event of a potential or actual incident. The procedures shall cover all potential types of security incident including system failures, errors resulting from incomplete or inaccurate data and confidentiality breaches. The procedures shall also include activities to perform for the effective gathering of evidence close to the time of the incident either for problem analysis and/or litigation. The procedures shall cover identifying the cause of an incident, implementing remedies to prevent recurrence, and communicating with users and others involved in a recovery situation.

2.0 INCIDENT RESOLUTION MANAGEMENT

2.1 INCIDENT RESPONSE PLAN

2.1.1 The Organisation shall have documented procedures to monitor and report all significant security events in line with the Incident Management Policy.

2.1.2 Recorded incidents shall be responded to in accordance with the Incident Response Procedure; Actions taken to recover from security breaches and to correct system failures shall be carefully and formally controlled in accordance with the Incidence Management Procedure. Suitable feedback processes shall be implemented to ensure that the people reporting the incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training.

2.1.3 Incident Management Procedures shall ensure that all security control violations are investigated promptly and that escalation procedures are invoked wherever necessary.

2.1.4 Reported incidents shall be analysed for trends; Incident logs shall be reviewed to detect any trends, which may identify risks to The Organisation. The analysis shall include:

- Identifying the cause of the incident.
- Assessing the impact of the incident; and
- Developing solutions to prevent the recurrence of the incident.

2.1.5 The methodology that was used to detect and resolve the incident shall be documented. This shall include the tools used for the forensic investigation.

2.1.6 The lessons learnt shall be documented and used to improve the Organisation's security posture.

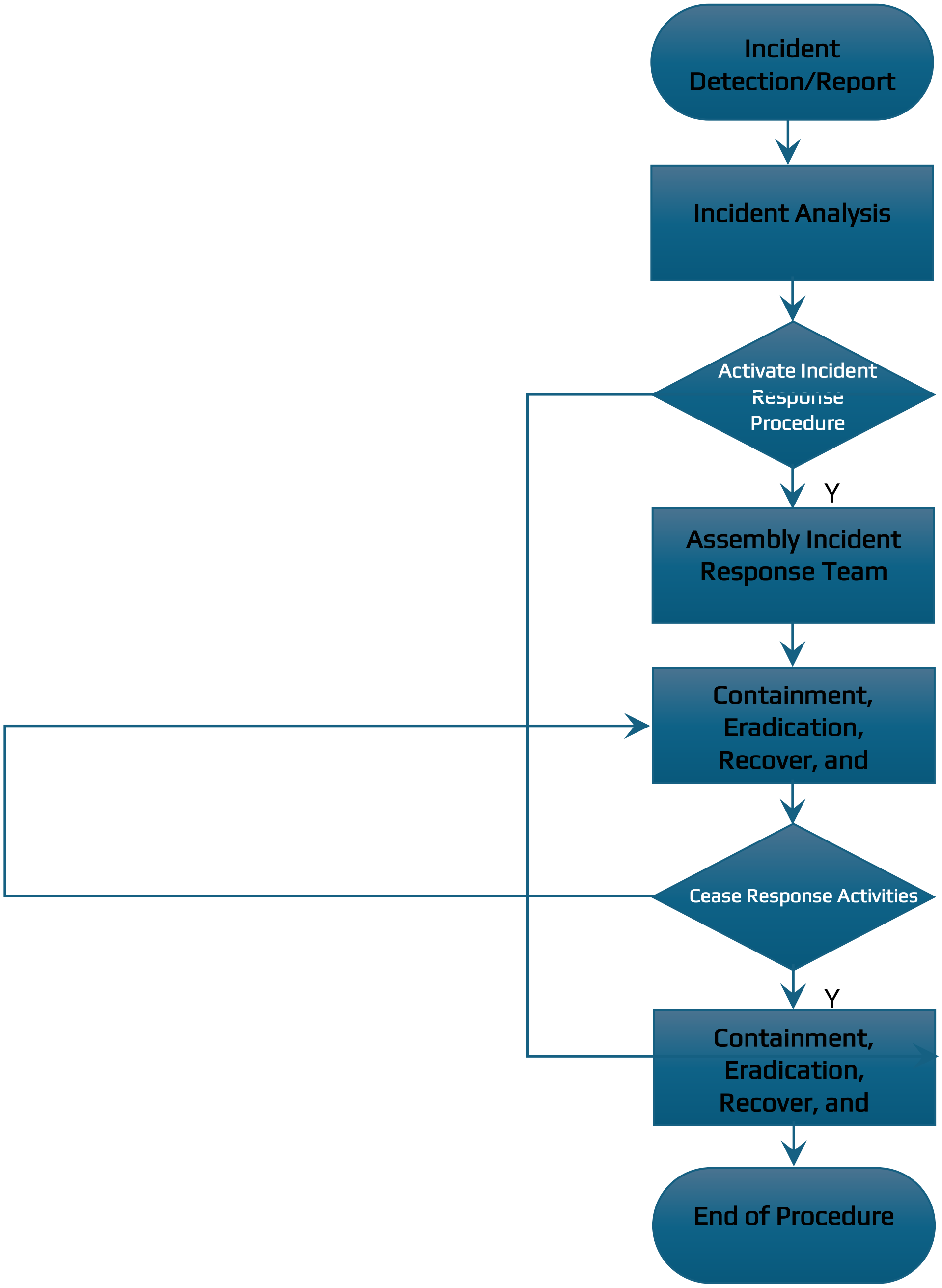
2.1.7 The Organisation shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

2.1.8 Unresolved incidents shall be reviewed and actioned; all unresolved security incidents shall be reviewed to ascertain what remedial action has been taken.

2.1.9 Critical incidents affecting the Organisation shall receive immediate attention. If required, the necessary actions shall be taken to isolate the affected areas; the isolation of affected areas is critical to The Organisation's business. This shall minimise the risk of unaffected areas being affected by the critical incident and decrease the overall impact on The Organisation's information resources.

2.2 INCIDENT RESPONSE PROCEDURE

The objective of this subsection is to ensure that incidents are efficiently resolved within stipulated timelines.


Incident Detection/Report
Incident Analysis
Activate Incident Response Procedure
Y
Y
Assembly Incident Response Team
Containment, Eradication, Recover, and
Cease Response Activities
Y
Containment, Eradication, Recover, and
End of Procedure

2.2.1 INCIDENT DETECTION AND REPORTING

An incident may be initially detected in a wide variety of ways and through different sources, depending on the nature and location of the incident i.e.

- Observation and report from internal user/staff
- Through routine monitoring activities
- Through external sources i.e., regulators, peers in the industry, threat intelligence, etc

Any occurrence of incident should be reported through the channels below:

- Escalate to xxxxx@yyyyyyyy.com for prompt reporting on an incident.
- Log the incident on the incident management portal.
- Escalate to your line manager if clarity/advice is required.

2.2.2 INCIDENT ANALYSIS

The incident response procedure must be started as quickly as possible after detection so that an effective response can be given. Once the incident has been detected, an initial impact assessment must be carried out to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on infrastructure
- The information assets (including personal data) that may be at risk or have been compromised.
- The likely duration of the incident i.e. when it may have begun.
- The business units affected and the extent of the impact to them.
- For breaches affecting personal data, the degree of risk to the rights and freedoms of the data subjects.
- Initial indication of the likely cause of the incident

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets (including personal data), business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

2.2.3 ACTIVATING THE INCIDENT RESPONSE PROCEDURE

Based on the outcome of the incident analysis, responsible individual/team for incident analysis should decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response Procedure and the convening of the Incident Response Team (IRT).

Guidelines for determining if a formal incident response should be initiated for any reported incident is as follows:

- There is significant actual or potential loss of classified information, including personal data.

- There is significant actual or potential disruption to business operations.
- There is significant risk to business reputation.
- Any other situation which may cause significant impact to the Organisation.

In the event of disagreement or uncertainty about whether to activate an incident response the decision of the Team Lead will be final.

If it is decided not to activate the procedure, then a plan should be created to allow for a lower-level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level.

If the incident warrants the activation of the IR procedure the Team Leader will start to assemble the IRT.

2.2.3.1 ASSEMBLE INCIDENT RESPONSE TEAM

Once the decision has been made to activate the incident response procedure, the Team Leader will ensure that all role holders (or their deputies if main role holders are uncontactable) are contacted, made aware of the nature of the incident, and asked to assemble at an appropriate location.

2.2.3.2 INCIDENT RESPONSE TEAM MEMBERS

The Incident Response Team will generally consist of the following people in the roles specified (or as designated by the Organisation), although the exact make-up of the team will vary according to the nature of the incident.

Team Member (Names)	**Designation**
XXXXX	Head, HR
XXXXX	Head, Information Technology/CIO
XXXXX	Head, Information Security/ CISO
XXXXX	XXXXX
XXXXX	XXXXX

Types of Incidents

Incident	Prevention/Mitigations	Improvement
Fire	● Fire evacuation drill. ● Fire Extinguishers, Fire Alarms, Smoke detectors. ● Call tree	Fire evacuation report, Internal reports, Business Continuity Plans
Flood	● Evacuation ● Call tree	Monitoring events/ news/ awareness through the media
Cyber attack	● Fire wall. ● Data encryption ● Anti-virus ● Vulnerability assessment	Constant updates and application of patches; network monitoring
Technology Outage	● Backup ISP ● Backup Servers ● Disaster Recovery	Disaster Recovery Tests
Sabotage	● Physical security ● CCTV, ● Access control into the ● building and offices	Constant training of staff and security personnel
Utility Outage	● Backup generator ● Inverter	Scheduled maintenance
Terrorism	● Physical security ● CCTV ● Access control into the building and offices ● Call tree	Monitoring events/ news/ awareness through the media, training of staff and security personnel
Reputational Damage	● Monitoring of Social sites ● Training of selected members of staff ● Staff awareness	Crisis Communication Policy
Civil Disorder	● Physical security ● CCTV ● Access control into the building and offices ● Call tree	Monitoring events/ news/ awareness through the media, training of security personnel, maintain good relationship with trade union.

2.3.3 INCIDENT MANAGEMENT, MONITORING AND COMMUNICATION

Once an appropriate response to the incident has been identified and the relevant business continuity plans activated, the Incident Management Team (IMT) needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

2.3.4 INCIDENT RESPONSE PLAN

The objectives of this incident response plan are to:

- Provide a concise overview of how the Organisation will respond to a disruptive incident affecting its business continuity.
- Set out who will respond to an incident and how our business continuity plans will be invoked.
- Describe the facilities that are in place to help with the management of the incident.
- Define how decisions will be taken about the response to an incident.
- Explain how communication within the Organisation and with external parties will be handled.
- Provide contact details for key people and external agencies.
- Define what will happen once the incident is resolved, and the responders are stood down.

2.3.5 INCIDENT DETECTION AND NOTIFICATION

2.2.5.1 INCIDENT DETECTION

The incident may be initially detected in a wide variety of ways and through different sources **(including emergency services),** depending on the nature and location of the incident. All incidents detected should be reported to the Incident Response Team. The incident response procedure is then started as quickly as possible so that an effective response is given.

2.3.5.2 INCIDENT NOTIFICATION

The following contacts will act as initial responders for a disruptive incident. Any of these contacts may be notified of an incident. They all have the authority to contact the Incident Response Team Leader at any time to ask him/her to assess whether the Incident Response Procedure should be activated.

Contact	Department	Phone number	Availability
Incident Response Team			
xxx	xxxx	xxxxxxxxxx	xx hours daily
xxx	xxxx	xxxxxxxxxx	xx hours daily
xxx	xxxx	xxxxxxxxxx	xx hours daily
xxx	xxxx	xxxxxxxxxx	xx hours daily

2.3.6 RECORDING THE INCIDENT DETAILS

On receiving notification of a possible disruptive incident, the person taking the call should record the details given, including:

- The name of the caller (the person reporting the incident)
- Caller's contact details
- Date and time of the call.
- Call taker's name.
- Exact description of the incident, including:
- Date and time of the incident.
- Nature of the incident e.g. fire, flood, explosion
- Location of the incident
- Whether emergency services have been called (if appropriate) and if so, are they in attendance?
- Any injuries or loss of life if known.
- An estimate of the scale of the impact
- Any other relevant information available.

2.3.7 CONTACTING THE INCIDENT RESPONSE TEAM LEADER

The **initial responder** to the incident should then contact the Incident Response Team Leader (or nominated deputy) using the contact details below to convey the above information.

Name	Role in Plan	Home Number	Mobile Number
xxxxxx	***xxxxxx***	***xxxxxxx***	***xxxxxxxx***

If none of the above can be contacted, the initial responder has the authority to decide whether or not the Incident Response Plan should be activated.

2.3.8 ACTIVATING THE INCIDENT RESPONSE PROCEDURE

Once notified of an incident the Team Leader must decide whether **the scale and actual potential impact of the incident justifies the activation of the Incident Response Procedure** and the convening of the Incident Response Team.

Guidelines for whether a formal incident response should be initiated for any incident of which the Team Leader has been notified are as follows.

- There is significant actual or potential danger to life

  OR

- There is significant actual or potential disruption to business operations

  OR

- Any other situation which may cause significant impact to the Organisation

Guidelines for the definition of **"significant"** within the above criteria are as follows:

- Loss of more than one day's business operation
- Service failure affecting all customers and staff
- Damage to reputation via coverage in national and international press
- Service failure affecting the performance of other services within The Organisation
- Regulatory sanctions with risk to license

The level of impact that should trigger the incident response procedure and the Business Continuity Plan is shown in the figure below.

- In the event of disagreement or uncertainty about whether to activate an incident response the decision of the Team Leader will be final.
- If it is decided not to activate the procedure, then a plan should be created to allow for a lower-level response to the incident within normal management channels. This may involve the invocation of a business continuity procedure at a local level.
- If the incident warrants the activation of the Incident Response procedure the Team Leader will start to assemble the IRT as described in the next section.

2.3.9 ASSEMBLING THE INCIDENT RESPONSE TEAM

Once the decision has been made to activate the incident response procedure, the Team Leader (or deputy) will ensure that all role holders (or their deputies if main role holders are unavailable) are contacted, made aware of the nature of the incident, and asked to assemble at the Incident Command Centre. The exception is the Incident Liaison (Facility Managers or other designated staff) who will be asked to attend the location of the incident to start to gather information for the impact assessment that the IRT will conduct so that an appropriate response can be determined.

2.3.10 ROLES AND RESPONSIBILITIES IN THE COMMAND CENTRE

2.3.10.1 INCIDENT RESPONSE TEAM MEMBERS:

The Incident Response Team (IRT) will consist of the following people in the roles specified.

Name	Role in Plan	Mobile Number
xxxxxx	***xxxxxxxx***	***xxxxxxxxxx***
xxxxxx	***xxxxxxxx***	***xxxxxxxxxx***
xxxxxx	***xxxxxxxx***	***xxxxxxxxxx***
xxxxxx	***xxxxxxxx***	***xxxxxxxxxx***

2.3.10.2 IRT: ROLES AND RESPONSIBILITIES

a) Team Leader

- Decides whether to initiate a response.
- Assembles the incident response team.
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement

b) Team Facilitator

- Supports the incident response team.
- Co-ordinates resources within the command centre
- Prepares for meetings and takes record of actions and decisions.
- Briefs team members on latest status on their return to the command centre
- Facilitates communication via email, fax, telephone, or other methods.

- Monitors external information feeds such as weather and news.

c) Incident Liaison

- Attend the site of the incident as quickly as possible.
- Assesses the extent and impact of the incident.
- Provides first-person accounts of the situation to the IRT.
- Liaises with the IRT on an on-going basis to provide updates and answer any questions required for decision-making by the IRT.

d) Business Operations

- Contributes to decision-making based on knowledge of business operations, products, and services.
- Briefs other members of the team on operational issues
- Helps to assess likely impact on customers of the Organisation.

e) Health and Safety

- Assesses the risk to life and limb of the incident.
- Ensures that legal responsibilities for health and safety are always met.
- Liaises with emergency services such as police, fire and medical.
- Considers environmental issues with respect to the incident.

f) Human Resources

- Assesses and advises on HR policy and employment contract matters.
- Represents the interests of Organisation employees.
- Advises on capability and disciplinary issues.

g) Communications

- Responsible for ensuring internal communications are effective.
- Decides the level, frequency, and content of communications with external parties such as the media.
- Defines approach to keeping affected parties informed e.g., customers, shareholders.

h) Legal and Regulatory

- Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks.
- Assesses the actual and potential legal implications of the incident and subsequent actions.

2.3.10.3 INCIDENT COMMAND CENTRE

The Incident Command Center creates a mechanism to coordinate all the steps taken to respond to an event and create a record of those actions to protect employees, infrastructure, and shareholder value. This includes:

- Communication and Intelligence.
- Command and Control.
- Coordination and Documentation.

Address: XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Location: XXXXXXXXXXXXXXXXXXXXXXXXXXX

2.4 BUSINESS CONTINUITY PLAN ACTIVATION

Once the IRT has been assembled at the command centre and as much detail as possible has been collected about the incident and its impact, a decision needs to be made about the most appropriate response.

These plans are as follows:

Plan title	Plan Description	Plan Owner
Restoration Plan	Business recovery plans	Head of Dept.
Technology Recovery Plan	Initiating and implementing the IT Disaster Recovery process for IT	Head of technology
Crisis Management Plan	Loss of physical access to branch locations or business units' location	BCM Manager
Vendor Management	Loss of services provided by a vendor or external service provider	Finance

Plan title	Plan Description	Plan Owner
Training Awareness & Competence Plan	Training of staff and interested stakeholders	BCM Manager
Exercise & Test	Testing of the BCMS	BCM Manager

Based on the current understanding of the business activities affected by the incident, an appropriate combination of the above business continuity plans should be activated to try to mitigate the impact. The method of activation of each plan is detailed in the individual plan document.

2.4.1 INCIDENT MANAGEMENT, MONITORING AND COMMUNICATION

Once an appropriate response to the incident has been identified and the relevant business continuity plans activated, the IRT needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

Regular IRT meetings must be held at an appropriate frequency decided by the Team Leader. The purpose of these meetings is to ensure that recovery resources are managed effectively and that key decisions are made promptly, based on adequate information. Each meeting will be minute by the Team Facilitator.

The Incident Liaison will provide updates to the IRT to a frequency decided by the Team Leader. These updates should be coordinated with the IRT meetings so that the latest information is available for each meeting.

2.4.1 COMMUNICATION PLAN

It is vital that effective communications are maintained between all parties involved in the incident response.

2.4.1.1 MEANS OF COMMUNICATION

The primary means of communication during an incident will be telephone, both landline and mobile. In the event of telephone communications being unavailable provision may be made for the use of radio communications, although the usable range of such equipment should be assessed. Email should not be used unless telephone and equivalent alternatives are unavailable.

2.4.1.2 COMMUNICATION GUIDELINES

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation.
- Advise internal team members of the need to refer information requests to the IRT.
- If the call is answered by someone other than the contact:
- Ask if the contact is available elsewhere.
- If they cannot be contacted leave a message to contact, you on a given number.
- Do not provide details of the Incident.
- Always document call time details, responses, and actions
- All communications should be clearly and accurately recorded.

2.4.1.3 INTERNAL COMMUNICATION

Calls to the Incident Response Team should use the main number which is: xxxxxxxx

Control Room

Number: xxxxxxxx

If there is no answer a message may be left. If the call is urgent the caller should both leave a message and call back as well as trying alternative methods of communication if available.

If leaving a message, ensure you leave:

- Your name
- Your number
- Your department/unit
- The name of the person the message is for
- The message

Outline Script:

My name is **[First name, Last name].** My telephone number is **[Mobile Number]** and I am calling from Organisation **[Location].** This message is for **[First name, Last name].** Kindly inform him that he/she should contact me urgently on **[Mobile Number**].

2.4.1.4 EXTERNAL COMMUNICATION

Depending on the incident there may be a variety of external parties that will be communicated with during the response. It is important that the information released to third parties is managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) should be passed to the member of the IRT responsible for communications.

Emergency responders such as the police, fire and ambulance services will be well practised in incident handling and will have their own structured methods for communication and every effort should be made to comply with these.

There may be several external parties who, whilst not directly involved in the incident, may be affected by it, and need to be alerted to this fact. These may include:

- Customers
- Vendors
- Shareholders
- Regulatory bodies

The Communications IRT member should make a list of such interested parties and define the message that is to be given to them. Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in the message log and passed to the Communications member of IRT.

There are several national and regional risk advisory systems which may be able to provide information about the incident and likely developments.

The following such systems are monitored:

External Agency	Dependency	Comments
National Emergency Management Agency	Emergency Response	Emergency: xxxxxxxxx
Federal Fire Service	Emergency Response	Emergency: xxxxxxx for Fire Outbreak. Call xxxxxxxx for Flood. Call xxxxxxxx for Collapsed Building
Country Police Force	Emergency Response	xxxxxxxx

The frequency of monitoring these systems should be increased for those that are directly relevant to the incident in hand. All relevant warnings should be logged and communicated to the IRT Team Leader.

2.4.1.5 COMMUNICATION WITH MEDIA

In general, the communication strategy with respect to the media will be to issue regular updates via top management. No members of staff should give an interview with the media unless this is pre-Authorised by the IRT.

The preferred interface with the media will be to issue pre-written press releases. In exceptional circumstances a press conference will be held to answer questions about the incident and its effects. It is the responsibility of the Communications IRT member to arrange the venue for these and to liaise with press that may wish to attend.

In drafting a statement for the media, the following guidelines should be observed:

- Personal information should be always protected.
- Stick to the facts and do not speculate about the incident or its cause.
- Ensure legal advice is obtained prior to any statements being issued.
- Try to pre-empt questions that may reasonably be asked.
- Emphasize that a prepared response has been activated and that everything possible is being done.

The following members of staff are appointed spokespeople for the Organisation if further information is to be issued e.g. at a press conference:

Name	Role	Incident Scale
xxxxxxxxx	xxxxxxxxx	xxxxx

The most appropriate spokesperson will depend upon the scale of the incident and its effect on customers, supplier, the public and other stakeholders. At any point in time, the MD/CEO will notify the <<responsible stakeholder>> for the release of any statement to the media.

2.5 CEASING RESPONSE ACTIVITIES AND STANDING DOWN

The Team Leader will decide, based on the latest information from the Incident Liaison and other members of the team, the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of business continuity plans may continue beyond this point but under less formal management control.

This decision will be up to the Team Leader's judgement but should be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable.

- The pace of change of the situation has slowed to a point where few decisions are required.
- The appropriate response is well underway and business continuity plans are progressing to schedule.
- Affected business activities have been resumed although perhaps at a lower level than normal.
- The degree of risk to the business has lessened to an acceptable point.
- Immediate legal and regulatory responsibilities have been fulfilled.

If recovery from the incident is on-going the Team Leader should define the next actions to be taken. These may include:

- Less frequent meetings of the IRT e.g. weekly depending on the circumstances.
- Informing all involved parties that the IRT is standing down.
- Ensuring that all documentation of the incident is secured.
- Requesting that all staff not involved in further work to return to normal duties.
- Returning the command centre to a state where it may be used for a future incident.

All actions taken as part of standing down should be recorded.

2.6 DEBRIEF AND POST INCIDENT REVIEW

After the IRT has been stood down the Team Leader will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to ensure that they reflect actual events and represent a complete and accurate record of the incident.

Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident. As input to this review the Team Leader will complete a Post Incident Report.

2.7 RECOMMENDATIONS/ADVISORY ON INCIDENT MANAGEMENT

Organisations with 1 – 5 Staff	Organisations with 6 – 20 Staff	Organisations with more than 20 Staff
● Consider the use of Excel document for incident management (Refer to Template – Incident Management) ● The different roles, teams or stakeholders can be combined based on the available staff strength	● Consider the use of Excel document for incident management (Refer to Template – Incident Management) ● Consider the use of open-source ticketing applications for incident management. https://osticket.com/ https://freescout.net/ ● The different roles, teams or stakeholders can be combined based on the available staff strength	● Consider the use of Excel document for incident management (Refer to Template – Incident Management) ● Consider the use of open-source ticketing applications for incident management. https://osticket.com/ https://freescout.net/ ● Consider the use of enterprise applications for incident management. https://www.freshworks.com/ https://www.manageengine.com/help-desk-software.html https://zammad.com/en ● The different roles, teams or stakeholders can be combined based on the available staff strength. However, it is encouraged that the teams identified in the poly are established.