Australian Government
Department of Industry, Science and Resources

Incident Management Framework

Contents

Administration

Endorsement

Version	Date	Endorsed by

Document History

Version	Date	Updated By	Purpose

Review Schedule

This Framework will be reviewed and updated annually.

Purpose

The purpose of the Incident Management Framework is to provide a structured and coordinated approach to incidents that could potentially disrupt the department's operations, reputation, or ability to deliver services.

This framework outlines the roles and responsibilities of those involved in the lifecycle of an incident. It also defines communication protocols for notifying stakeholders, as well as procedures for initiating backup and recovery measures, conducting post-incident reviews, and updating the framework based on lessons learned.

Having a well-defined incident management function in place can help the department to minimise the impact of ICT incidents, reduce downtime, and facilitate a faster and more effective response. It will also provide assurance to stakeholders that the department is prepared to handle unexpected ICT disruptions and maintain business continuity.

The intended audience of this framework are internal staff and vendors that may engage in the incident management function.

Incident Management Contact Details

Chief Information Officer Division, ICT Operations Branch, IT Service Management Section

Email: s22

A/H On Call Phone: s22

Scope

The role of this document is to:

1. Define an ICT incident,
2. Provide a structured and coordinated approach to detect, respond, and recover from ICT incidents,
3. Define roles and responsibilities associated with the management of an incident,
4. Minimise the impact of an incident and improve the recovery response time, and
5. Initiate Post-Incident Reviews (PIR) to determine the root cause.

ICT Incident Management Terms & Definitions

Term	Definition
CDSS	Corporate and Digital Support Services
CIO	Chief Information Officer
CIOD	Chief Information Officer Division
Degraded	Intermittent issues and reduced quality of service. A workaround may be available.
Department	Department of Industry, Science, and Resources (DISR)
DISR	Department of Industry, Science, and Resources
DR	Disaster Recovery, which is defined as a critical ICT disruption which causes (or has the potential to) significant business impact or reputational damage to the department.
ICT	Information and Communication Technology
Incident	An unexpected event that disrupts business operation or reduces the quality of an ICT service.
IVR	Interactive Voice Response is an automated telephone system that combines pre-recorded message.
Major Incident	An incident that affects business-critical services or impacts many users.
MIM	Major Incident Manager
Outage	A planned or unplanned loss of service.
PIR	A Post Incident Review evaluates the response activities, identify areas for improvement to prevent or mitigate future incidents.
Problem	A cause or potential cause of one or more Incidents. It is often an underlying fault which may have led to one or more incidents.
Request	A Service Request, a pre-defined formal request for help or access to an IT service. Examples include asking for a new laptop, onboarding an employee, or requesting a password reset.
RFC	Request for Change
Tech bridge	A tech bridge is a communication channel set up to allow technical experts and other stakeholders to discuss and troubleshoot an issue.
Vendor	An external service provider who offers IT services to the department. For e.g., Microsoft, Aurion etc.

Roles and Responsibilities

Incident Manager

s47E(d)

s47E(d)

Note: s47E(d)

Major Incident Manager (MIM)

s47E(d)

Note: s47E(d)

Technical Areas

s47E(d)

CDSS Management

s47E(d)

CDSS Analyst

s47E(d)

Senior ICT Ops Management

s47E(d)

Commented [TB1]: Need to rename this

Commented [TM2]: Not sure if we need this section

Major Incident Management RACI

Commented [MT3]: RACI from MIM Process Doc

RACI (Responsible, Accountable, Consulted, and Informed) is a responsibility assignment matrix. The Major Incident RACI defines the roles and responsibilities of all parties involved in a major incident response.

These have been listed in the table below:

s47E(d)

Commented [TB4]: What happens out of business hours? Is that where the retrospective change comes in?

s47E(d)

Commented [TB5]: I don't think we have this one

Definition	Key
Responsible: For the activity.	R
Accountable: For ensuring that the activity is completed.	A
Consulted: Requires two-way discussion on topic.	C
Informed: Required to be kept informed of the status until resolved.	I

Note

s47E(d)

3. Communication Strategy

During a major incident it is important to communicate clearly with stakeholders and the support teams about the status of the incident, estimated time to resolution or resolution of the incident. These communications should be meaningful to all parties involved.

Clear and meaningful communication should ensure that:

- Stakeholder impact is clearly stated.
- The department is alerted to the impacted service.
- Staff are provided workarounds, if available, and any support options.

s47E(d)

Communication Channels

s47E(d)

s47E(d)

s47E(d)

s47E(d)

Service Level Agreements for Communication

s47E(d)

s47E(d)

s47E(d)

s47E(d)

ICT Incidents

s47E(d)

Minor Incident

s47E(d)

Major Incident

s47E(d)

s47E(d)

Incident severity

s47E(d)

s47E(d)

s47E(d)

s47E(d)

s47E(d)

When to raise an incident

- s47E(d)

Service Level Agreement Based on Priority

s47E(d)

s47E(d)

Note: Unless otherwise specified, the department's business hours are 8:00am - 5:00pm, Monday – Friday AEST/AEDT; Official public holidays are not considered business hours.

Parent and child incidents

s47E(d)

Parent Incident

s47E(d)

s47E(d)

Child Incident

s47E(d)

s47E(d)

Major Incident Management Process

s47E(d)

s47E(d)

Commented [MT6]: Taken from MIM Process Doc

Commented [TB9]: Need to decide whether it is Group or Team for consistency.

Commented [MT10R9]: I think Technical Team would be best

Commented [TB7]: Update link

Commented [MT8R7]: Link updated

Commented [CK11]: Need to clarify between IM and MIM

s47E(d)

s47E(d)

s47E(d)

s47E(d)

s47E(d)

Major Incident Resolution

s47E(d)

Raising Changes to resolve a Major Incident

s47E(d)

Commented [TB12]: Need to revisit this.

Commented [CK13]: Just note here something about Emergency/ LTW type changes

Commented [TB14]: Need to revisit this as well.

Post-Incident Review (PIR)

Commented [MT15]: Taken from MIM Process Doc

s47E(d)

s47E(d)

Problem and Knowledge Management

s47E(d)

Commented [T[16]]: Probably doesn't need to be here if it's already in another doc?

Commented [TM17]: Worth having but would need to mature PM to have correct info in here

Commented [TB18]: Should this go into a definition section?

Reporting

Reporting metrics

Appendices

s47E(d)

Commented [TB19]: Need to update the link

Commented [MT20R19]: Link updated