ACT Government | ACT Health

ICT Incident Management Procedure

Document number	**AHDPD-12:2022**
Effective date	12 September 2022
Review date	12 September 2025
Author branch	Digital Solutions Division, Technology Operations Branch
Endorsed by	Chief Information Officer
Audience	All members within the Division
Version number	1.1

Contents

Purpose

The ICT Incident Management Procedure will introduce and define the process framework including the workflow, roles and procedures required to support business operations in the event of an incident.

Scope

This document defines the incident management process and will touch on components of other IT Service Management processes though will not define other processes in any degree of detail.

Incident Management Overview

ICT Incident Definition

An ICT incident is any unplanned interruption to an IT service, or reduction in the quality of an IT service, or associated infrastructure.

Incident Management Objectives

The primary goal and objective of incident management is to restore normal service operation as quickly as possible and to minimise the adverse impact on business operations.

Incident management can be applied to any event which either disrupts or has the potential to disrupt a service. This includes events which are communicated directly by users through the Digital Solutions Support (DSS) service desk, or Digital, Data and Technology Services (DDTS) service desk, or by Digital Solutions Division (DSD) level 2 staff, or if an incident is identified and reported from NTT or DDTS level 3 staff.

Incident Management Roles and Responsibilities

Role	Description
DSD Incident Manager	Responsible for the procedure and for the day-to-day management of the procedure. The manager will take a proactive approach and undertake continuous actions and monitoring to ensure that incidents and potential incidents are dealt with in a timely manner. The Incident manager will assist Level 1, Level 2 and Level 3 support where applicable with the management of an incident. Will help facilitate the updates and notifications throughout an incident as well as the maintenance and circulation of all associated incident reports and records to relevant governance committees.
Incident Owner	Responsible for ensuring that all activities defined within the practice are undertaken and that the practice achieves its goals and objectives. With the assistance of the Incident Manager, release the updates and notifications throughout an incident where applicable. Typically a System Administrator under Level 2 Support.
End User	The End User is the person using an IT resource. This role is responsible to report all Incidents and make all IT requests and contacts through DSS.
IT Staff	Any IT staff from the IT organisation. This role is responsible for the IT infrastructure and the delivery of IT Services.
Assistant Director, DSS	The Assistant Director, DSS is responsible for the day-to-day management of DSS and assisting with the management of escalated issues.
Digital Solutions Support (DSS)	Digital Solutions Support is responsible for the day-to-day communication with all End Users and to facilitate the resolution and fulfillment of Incidents and Requests. DSS forms Level 1 Support.
DSS Team Leader	DSS Team Leaders assist with escalation and prioritisation of incidents. During business hours they manage P4 and P3 incidents, and outside of business hours they manage all priorities until a more senior member is able to take over i.e., Senior Director On-call or Incident Manager.
Level 2 Support	Level 2 Support is responsible for handling Incidents that DSS cannot resolve. These group(s) are usually the Subject Matter Experts and typically have longer timescales to perform incident diagnosis and resolution tasks.
Level 3 Support	Level 3 Support is responsible for handling Incidents that require specialised and in-depth technical skills.
Level 3 Incident Management Team	An individual or group of individuals identified by DDTS and NTT as responsible resources for incident management where systems are hosted and supported by the relevant organisation.
Stakeholder/s	Stakeholders are key members within our organisation that has a need to know when an incident is raised and what the status of it is. Stakeholders encompass a large number or business areas, from identified executives within Canberra Health Services (CHS) and North Canberra Hospital (NCH) to leadership groups from impacted business areas. The stakeholders directly involved or impacted by this SOP are the following: DSD Executive Branch Manager (EBM), DSD Chief Information Officer (CIO), CHS CIO and the NCH Operations Manager.

Table 1 - Incident Management Roles & Responsibilities

Procedure Summary

This section summarises the activities associated with each stage of incident management.

The Detailed Procedure section steps through each stage and activity in more detail, providing a greater degree of definitions for the expected roles and responsibilities and details the action required.

1. Incident Identification and Prioritisation

1.1 Incident Identification

An initial call or identification of an incident needs to occur, an incident is defined as an IT service that is not functioning or not functioning at an acceptable level.

1.2 Logging an Incident

DSS is responsible for registering all customer queries, requests, and issues in JIRA Service Management (JIRA). An incident may also be recorded in JIRA by the DSD Incident Manager or Level 2 Support.

The incident record will include customer details, including name, systems, services, and physical locations impacted, contact details and any relevant information associated with the incident.

DSS is open 24 hours a day on a rotating roster. This is inclusive of weekends and public holidays. For Level 2 working times please see 2.1.

DSS can be contacted by calling 02 5124 5000, raising an online request via the Jira Customer Portal or by emailing digital.support@act.gov.au. All urgent incidents emailed to DSS should be escalated by phone to ensure priority is assigned as quickly as possible.

1.3 Incident Prioritisation

DSS, the DSD Incident Manager or Level 2 Support will assess the incident and determine a priority for the incident. DSS and Level 2 support are able to set an incident as a P4 or P3, however formal engagement with the Incident Manager or Senior Director is required for P2 and P1 incidents.

P4s are the lowest priority while P1s are the highest priority. The priority of an incident dictates how urgently it must be completed. P4 and P3 incidents are typically treated as business as usual while P1 and P2 incidents indicate a large-scale issue that requires immediate response. An incident's priority also determines it's Service Level Agreements and response targets.

The following table can be utilised to assist in determining the incident priority.
It is important to note that the priority can change throughout the incident based on criticality of the system, impact to stakeholders, clinical or political risk etc.

Incident Prioritisation Table

	P1 – Major Incident	P2 – High Priority Incident	P3 – Minor Incident	P4 – Minor Incident
ICT Description of Impact	Total system dysfunction and/or shut down of operations, severely impacting Government critical services	Disruption impacts effective delivery of business services of an entire site, which could impact other sites.	Disruption to a number of services or programs within a site, possible flow on to other sites.	Some disruption manageable by altered operational routine in a local site. Workarounds available.
CHS Description of Impact	A workaround is not available, and resolution is urgent, ability to deliver intended critical patient care is severely impacted. Patient or Staff safety has the potential to be impacted.	Ability to deliver critical patient care is seriously impacted. Directorate critical services cannot be delivered.	Limited ability to process transactions or access data critical to conducting business that may lead to patient care or financial concern.	Impact is limited to specific records and does not adversely impact patient care.
Scenario Examples	DHR is unavailable to all and BCP has to be activated. Loss of access to all Citrix systems as a result of network issues. A public facing system becomes inaccessible. Likely to have a reputational impact. Data centre fail, loss of network across multiple Health facilities. BCP has to be activated.	Messaging not flowing through rhapsody for multiple systems. Loss of access to a number of systems accessible via Citrix. A single system becomes inaccessible to all staff, may have reputational impact. Infrastructure in a health centre fails, requires team to replace.	Messaging not flowing through Rhapsody for a single system. Network degradation for a small number of individuals in a single location.	Access to training is unavailable for a user. A frozen session that requires a termination on Citrix. A staff member not being able to log into DHR.

Table 2 – Incident Prioritisation Table

2. Incident Diagnosis and Escalation

DSS or the Incident Owner will attempt to discover the full symptoms of the incident and determine the cause and possible resolution. A resolution may be found by referencing knowledge base articles, or by referring to previously logged JIRA or SerivceNow tickets.

If a resolution is found, the incident can be resolved; otherwise, it will be escalated for investigation. If escalated the user is informed of this fact and is provided the incident ticket number.

2.1 Escalating an Incident to Level 2 Support

If an incident cannot be resolved by DSS they will escalate the incident to the appropriate Level 2 Support team.

The Level 2 support team is then responsible for the investigation and resolution of the incident as part of the incident lifecycle. One of the Level 2 system administrators will then take up the role of Incident Owner and be the primary contact throughout the incident.

The escalation process is initiated to ensure there is adequate notification and follow-up of incidents, resulting in quick resolution within agreed service targets.[Table 3]

Standard business hours for Level 2 and the greater ACT Health workforce is from 8:30AM to 5:00PM, with some slight variance on either side. If escalations are required to level 2 teams outside of this period, please consider viewing their on-call rosters for assistance.

2.2 Investigation and Diagnosis

The Incident Owner will investigate and diagnose the incident to understand all relevant details of the incident.

This can include establishing exactly what has gone wrong; the chronological order of events; confirming full impact of the incident including number of users affected; identifying any events that could have triggered the incident (e.g., a recent change, server patching or user action); and performing detailed searches of previous incidents or problems, internal and vendor knowledge databases or available error logs.

Once the potential resolution has been identified, the actions to be undertaken to resolve should be applied. This may require asking the End User to follow or perform certain activities (e.g., restarting failed service, remote control session of user's computer etc) or engaging with Level 3 support, third-party vendor/s or other technical resources to perform activities.

2.3 Escalating to Incident Management Team

Certain incidents may require escalation through the Incident Management Team for several reasons.
This may include incidents reported by executive or otherwise VIP users, if an incident appears to be taking too long to resolve, if a major incident occurs, if an incident is nearing a breach of an SLA, if an incident involves sensitive or confidential matters, or if the receiving Analyst or Incident Owner feels the standard incident workflow is insufficient to resolve the incident.

In these cases, the Incident Management Team will make best judgement on how the incident will flow to resolution; ensuring incident management process is followed and best practices applied while aiming for the most efficient resolution.

The Incident Management Team may activate the emergency management process and engage directly with the Level 3 Incident Management Team.

If an escalation is being requested from a Level 2 or Level 3 Support Team, then an impact statement covering severity and criticality, size of affected userbase, and potential clinical implications is required for responsive actioning.

Response and Fix Targets

Response and Fix targets have been determined to give an outline on the expected resolution time for each priority level.

These targets are designed to ensure that we are responsive to our clients in ensuring swift resolution to incidents. It will be noted that the response and fix targets are a guide for incidents within a certain team's space and should an incident cross streams then the targets are paused until troubleshooting returns to the responsible team.

An example would be when logging an Incident with DSD, if a P3 ticket were to be handed to DDTS, then the 8-hour fix target for DSD will pause whilst DDTS's 2-week target will then be applied. In turn, once it returns to DSD that timer will resume.

	Group	Response Target	Resolution Target
1	DSD	5 mins	4 hours
	DDTS	30 mins	4 hours
	NTT	30 mins	2 hours
2	DSD	10 mins	4 hours
	DDTS	1 hour	2 business days
	NTT	30 mins	2 hours
3	DSD	30 mins	8 hours
	DDTS	3 hours	2 weeks
	NTT	2 hours	1 business day
4	DSD	30 mins	8 hours
	DDTS	5 hours	1 month
	NTT	1 business day	4 business days

Table 3 –Response and Fix Targets

Sources: Shared Services ICT Incident Management Fact Sheet, Level 3 Support – Response and Fix Targets KB Article

3. Resolution, Recovery and Closure

3.1 Resolution

Once a resolution has been identified and tested as successful, the details leading to the successful resolution are recorded into JIRA. This information includes closure notes, closure code and the closure Configuration Items (CI) (e.g., the CI that was actually at fault).

The End User will be notified and confirmation of the acceptance of incident closure will be received. The incident will be marked as resolved.

3.2 Incident Closure

After 5 days of being in a resolved state, an incident will automatically be closed. At any time during the 5-day window, the user can indicate that they feel the resolution is inadequate or false. The user can do this by either responding to the closure email or by clicking the appropriate link sent to them in the resolution email. Alternatively, they can contact DSS and request for the incident to be reopened.

3.3 Post Incident Actions

Following a P1 or P2 incident a Post Incident Report (PIR) will need to be prepared and completed within 10 business days of the incident occurring. The PIR will be initialised by the Incident Manager and co-authored by the Incident Owner. Once its completed it will be recorded on the Incident Recommendations register.

The relevant Incident Owner, System Administrator or delegate is responsible for completing the technical aspects of a PIR. Once a PIR is completed by the Incident Owner, it is then to be reviewed by the relevant Senior Director for accuracy and transparency.

The Level 3 Incident Management Teams from DDTS or NTT is responsible for producing the PIR on P1 and P2 incidents that have been escalated to Incident Management for applications supported or hosted by the relevant organisation. The DSD Incident Manager is responsible for following up with both DDTS and NTT to ensure this is provided.

There will be times where both a technical and operational impact PIR will be required, these should be produced at the Incident Owner’s discretion or by direction from the DSD Incident Manager.

The PIR should be tabled at the next ACT Health Change Control Board (CCB) meeting. The Chair of the ACT Health CCB will determine whether or not the PIR needs to be escalated to any of the CHS or ACT Health committees.

Follow up actions should be assigned to an action officer and regularly reviewed by the Incident Manager.

Communication

Communication requirements will vary depending on the criticality of the impacted system, impact to stakeholders and priority of the incident.

Definitions are provided as per the following, expected application of these communication methods are detailed in the workflows and detailed procedure.

OpsGenie

OpsGenie is an Incident Management alerting tool developed by Atlassian which is currently used by DSD. OpsGenie is used for on-call scheduling and incident alerting. Incident alerts are sent to relevant stakeholders and technicians via email, SMS and/or automated voice message.

It is expected that an alert is raised for all P1 and P2 incidents, once the alert is raised, notifications are sent via the avenues listed above. Notes can then be left at every major milestone updating the stakeholders of the progress of the incident.

Best practice incident management communication will see an update to incident notification to occur once per hour or more frequent where there is a major step in the progress of the incident.

Opsgenie alerts are to be sent by the DSD Incident Manager during business hours and by the DSS Team leaders or Senior Directors out of business hours.

Statuspage

Statuspage is an outage notification tool developed by Atlassian which is currently used by DSD. It handles both scheduled downtime and unplanned outages.

Statuspage is used in conjunction with the all-staff email notifications that are sent out with outages. If an incident has a noticeable front-end impact, both an all-staff email and Statuspage notification will be released to inform staff.

Updates to the Statuspage are done once an hour at a minimum, or whenever there is a significant update to the outage.

The link to Statuspage can be found here.

Digital Solutions Operations Centre (DSOC) SMS Dashboard

The DSOC SMS Dashboard is a webtool designed to collect various SMS messaging that may relate to Incident Management. The dashboard is displayed within the DSOC Incident Response room and above all the monitors within DSS.

The dashboard collects SMS messages from the following sources: Opsgenie, DDTS's SMS Communications group, CHS Code SMS group, and Security's SMS alerting group.

A link to the dashboard can be found here.

Email notification – planned and unplanned outages

DSD have two different styles of templates used for email notifications which generally are associated with both planned and unplanned outages.

The red banner templates are used for emergency communications and tend to be most suited to P1 incidents or incidents that have been identified to have major impact to stakeholders.
The blue banner templates are used generally used for planned and unplanned outages that do not fit into the emergency category.

Both templates clearly articulate what is happening, when it happens, the potential impact and workarounds or information the stakeholder may need to consider.

If either template is required, then the Incident Manager can request Level 2 Support to draft the email for review. The Incident Manager will review the communications and then send it for approval to the Chief Information Officer (CIO)'s office. Once approval has been obtained, a Senior Director will need to send it out to the relevant distribution lists.
If email communications are required outside of business hours, then the on-call Senior Director is able to send communications without additional executive approval.

The communication templates are available on the DSD SharePoint page at the following link.
Additionally, some generic incident email templates have been created and can be found on confluence.

CHS Code Alerts – Code Yellow

DSD plays a pivotal role in communicating incidents and resolution timelines to CHS and NCH. This includes ensuring the appropriate business ICT representative is aware of an incident in a timely manner, keeping them up to date relating to ICT restoration. The appropriate ICT business representative will liaise with the initiation and management of the hospital's emergency management response.

CHS have appropriate emergency management response plans, and often the plan prescribes specific colour coded emergency categories. There are currently eight codes in place covering specific incidents at CHS facilities with the Code Yellow being utilised to escalate an internal disaster. NCH has 7 codes in place with Code Yellow being utilised as Internal Emergency.

Internal Disaster and Internal Emergency covers a range of categories with the most relevant to this procedure incorporating disruptive events to telecommunications and ICT systems, infrastructure, or electricity supply.
The escalation process allows for relevant stakeholders to be notified of a disruption or potential disruption to service in a timely manner.

Any ICT systems and infrastructure disruption may commence with an initiation and release of a code yellow or may necessitate an initiation to distribute a code yellow. This is completed by CHS.

More information is available on the Canberra Health Services Emergency plans and responses.

Executive and Technical Teams Chatrooms

In the event of a P1 or P2 outage, there may be a requirement for the Incident Manager to create a chatroom in Microsoft Teams to coordinate resources and relay information.

A MS Teams chat will be created to centralise the flow of information and resourcing for the incident investigation. This room will typically include Incident Manager(s), the technical resource required and the director or senior director at minimum. If additional resources are required, then they'll also be added to the chat as required.
These Teams chats will be named the following:
"Technical Room – PX – DSD-XXXXXX – Issue Description" where "PX" is the priority of the incident and "DSD-XXXXXX" is the ticket number. The Issue Description would be aligned with the title of the incident in Jira.

An executive MS Teams chat will be created when there's a requirement to provide more detailed live updates to any executive or key stakeholder. The Incident Manager and Senior Director of the affected system are also included within this executive channel.
The Incident Manager/Senior Director will be responsible for providing significant updates to the executives in-line with what Opsgenie provides. While Opsgenie alerts provide brief updates, the updates given to the executives will be more substantial and include a more detailed brief.

The initial creation of the Executive chatroom will include the following staff:

- DSD CIO
- CHS CIO
- NCH Operations Manager
- EBM, Technical Operations
- EGM, Digital Health Record
- EBM, Future Capability & Governance

An executive may invite other delegates or interested parties at their discretion.

The Incident Manager or Senior Director will provide updates to the executive board as they're received, typically relaying status updates from the technical to the executive chat. The two roles act as a conduit between the two channels to ensure that there is sufficient transparency between the two groups.

The Executive Teams chats will be named the following:
"Executive Room – PX – DSD-XXXXXX – Issue Description" similarly to how the Technical Rooms are named.

Health Incident Management Teams Channel

ACT Health has a Health Incident Management MS Teams channel. The purpose of this channel is for the Incident Manager to relay any outage to Level 2 support, and to act as another avenue of escalation for Level 2 support if they are unable to contact the Incident Manager via phone.

Incident Response Room

The ICT Incident Response Room is physically located at the DSOC at Bowes St. When activated the numerous wall mounted televisions will be utilised for incident management/monitoring and the large teleconference screen will be utilised for virtualising the incident room for stakeholders who are physically located in other buildings/areas of ACT.

The Incident Response Room is activated for all major Incidents which are commonly referred to as a Priority 1 or P1 incidents, there may also be other major incidents with which the room is utilised.

Once activated all relevant stakeholders, Executives and key representatives will be invited to attend physically or via the teleconference screen. DSS Senior Directors will ensure that any System Administrator working on the Incident will also be included in the teleconferences.

Updates will be shared in real-time as the incident investigation progresses.

Incident Management Engagement

Incidents assessed as a P1 or P2 during business hours must be escalated to the DSD Incident Manager by contacting the DSD Incident Manager on 02 5124 9867 and/or by posting a message and tagging the DSD Incident Manager in the incident management chat room on MS Teams.

If an incident occurs outside of business hours and there is the potential need for escalation, the incident will be reviewed by a DSS Team Leader for prioritisation and may require the assistance of the Senior Director on-call.

If an Incident were to carry over from business hours to out of hours, and vice versa, there is an expectation that the Incident Manager and/or the DSS Team Leader/s will provide a handover of the incident to the Senior Director on-call, including what actions have been taken.

Once an incident has been escalated, the DSD Incident Manager, DSS Team Leader/s or Senior Director on-call will liaise with DSS, Level 2 and/or Level 3 as required to ensure regular updates are available.

RACI Incident Communication Matrix

The following table is directed at Incident Management holistically. Variance may be present depending on what priority the incident is classified as. The following should therefore be used as a baseline and not form a definitive decision-making tree for communication/engagement.

The RACI Definitions are as follows:

- Responsible (R) - Those who do work to achieve the activity.
- Accountable (A) - The resource ultimately accountable for the completion of the task.
- Consulted (C) - Those whose opinions are sought. Two-way communication.
- Informed (I) - Need to be informed about the activity.

RACI Matrix for Incident Management

Process ID	Activity	DSS	Assistant Director, DSS	DSS Team Leaders	Support Level 2	Support Level 3	DSD Incident Manager	Incident Owner	End User	Level 3 Incident Management Team	Stakeholder/s
1.1	Incident identification	R	A	R/A	R/C	-	-	-	C	-	-
1.2	Logging an Incident	R	A	R/A	R/C	-	-	-	C	-	-
1.3	Incident Prioritisation	R	C	R/A	R	-	R/A	I	I	-	I
2.1	Escalating an Incident to Level 2 Support	R	A/C	R	I	-	R	R	I	-	I
2.2	Investigation and Diagnosis	-	-	I/C	C	C	I/C	R/A	C/I	-	C/I
N/A	Communications	-	I	C	R	R/C	C	A	I	C /I	I
2.3	Escalating to Incident Manager	R	I	A/C	R	R	A/C	R/C	I	C	C
3.1	Resolution	I	-	I	C	C	C/I	R	C	C /I	C
3.2	Incident Closure	I	-	I	R	-	I	R/A	I	C /I	I
3.3	Post Incident Actions	-	-	A	C	C	A	R	C/I	C	C/I

Table 4 – RACI Matrix for Incident Management

Detailed Procedure

This section looks at the workflow in detail, providing further guidance around the role involved and actions required.

It is important to note that the Incident Owner and/or DSD Incident Manager will at times need to apply a best practice approach to the workflow in order to achieve a positive outcome, this should not be at the detriment to the defined process.

Below are the names of each workflow and a brief introduction for each one.

Incident Lifecycle – Creation and Prioritisation

This workflow details the initial stage of the incident lifecycle. It's use is primarily to record the incident and determine the priority.

Incident Lifecycle – Minor (P3/P4) Incidents

This workflow details how a minor incident is handled at a high level. A minor incident is classed as either P4 or P3 and typically does not require any Incident Manager involvement.

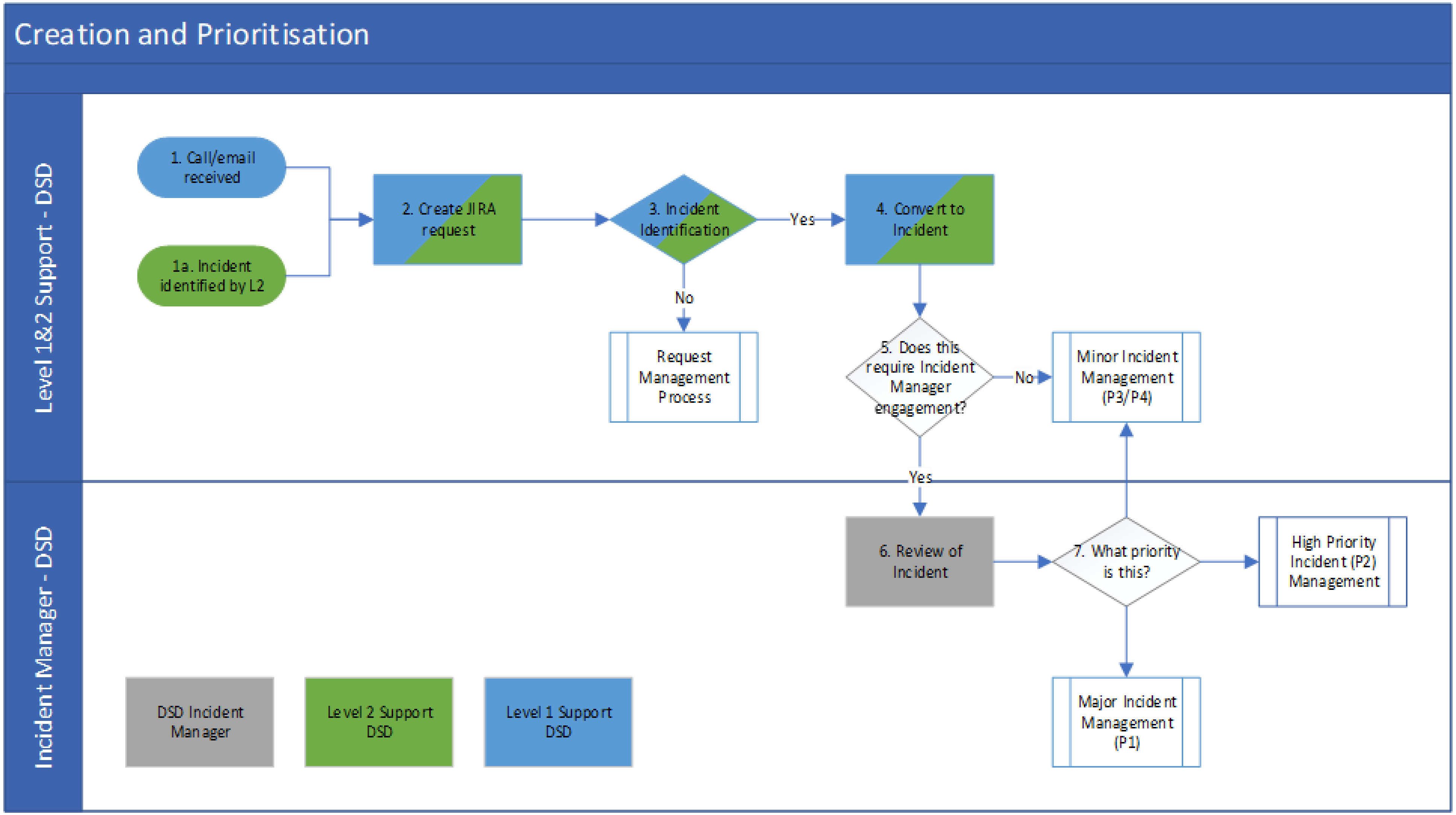
Incident Lifecycle – High Priority (P2) Incidents

This workflow details the management of P2 Incidents. It covers the escalation process and potential resourcing from Level 3 Support, and also shows the entry points for communications.

Incident Lifecycle – Major (P1) Incidents

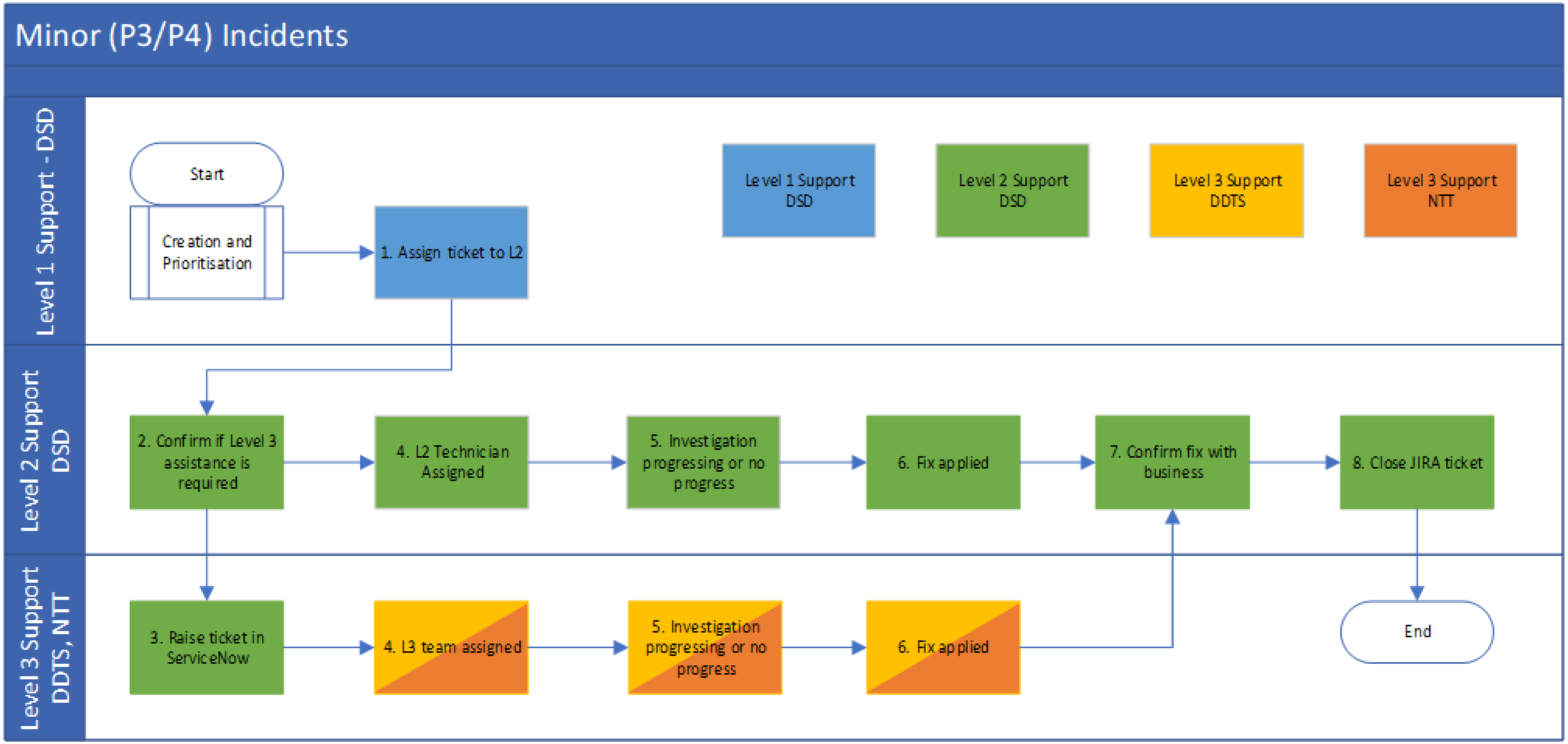
This workflow details the response for any major (P1) incidents that occur. A major incident is the highest category of impact for an incident.

Incident Lifecycle – Creation and Prioritisation


Creation and Prioritisation
Level 1&2 Support - DSD
Incident Manager - DSD
1. Call/email received
1a. Incident identified by L2
2. Create JIRA request
3. Incident Identification
Yes
No
4. Convert to Incident
Request Management Process
5. Does this require Incident Manager engagement?
No
Minor Incident Management (P3/P4)
Yes
6. Review of Incident
7. What priority is this?
High Priority Incident (P2) Management
Major Incident Management (P1)
DSD Incident Manager
Level 2 Support DSD
Level 1 Support DSD

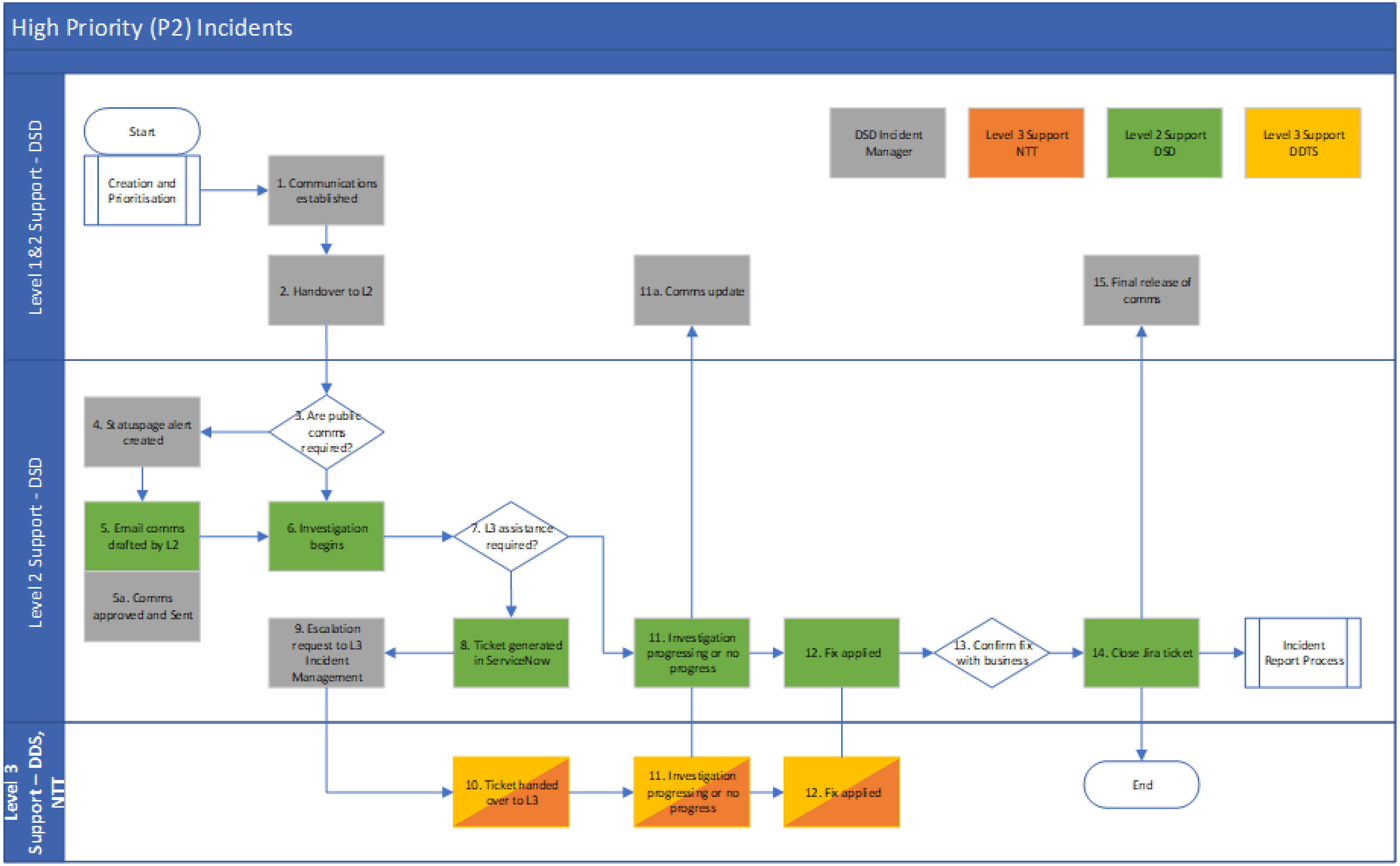
ID	Step	Description	Involved
1.	Call/email received	Call received by DSS from a client advising they have an issue with a system/their hardware. Email received to incoming queue advising there is an issue.	DSS End User
1a.	Incident Identified by L2	Incident proactively identified by L2 support	Level 2 Support
2.	Create Jira Request	DSS or L2 support to create a Jira ticket and input details of the incident.	DSS Level 2 Support
3.	Incident Identification	If raised by a call or email, DSS is required to review the information provided and troubleshoot the request from the client. If raised by Level 2, basic troubleshooting is required to determine if it's an incident. If the ticket is a Request, follow Request Management Process.	DSS Level 2 Support
4.	Convert to Incident	Once confirmed that ticket is an incident, convert the Jira ticket to one.	DSS Level 2 Support
5.	Does this require Incident Manager engagement?	Review of the incident to determine if this is requires a potential escalation or prioritisation. Liaise with the Incident Manager to confirm this.	DSS Level 2 Support DSD Incident Manager
6.	Review of Incident	Incident Manager reviews the incident and acquires more information from DSS or Level 2 Support.	DSD Incident Manager
7.	What priority is this?	Based off step 6, determine what priority the incident is. If it's a P4/P3 then follow the Minor Incident workflow. If it's a P2, follow the High Priority Incident workflow. If it's a P1, follow the Major Incident workflow.	DSD Incident Manager

Incident Lifecycle – Minor (P3/P4) Incidents


Minor (P3/P4) Incidents
Level 1 Support - DSD
Level 2 Support DSD
Level 3 Support DDTS, NTT
Start
Creation and Prioritisation
1. Assign ticket to L2
Level 1 Support DSD
Level 2 Support DSD
Level 3 Support DDTS
Level 3 Support NTT
2. Confirm if Level 3 assistance is required
4. L2 Technician Assigned
5. Investigation progressing or no progress
6. Fix applied
7. Confirm fix with business
8. Close JIRA ticket
3. Raise ticket in ServiceNow
4. L3 team assigned
5. Investigation progressing or no progress
6. Fix applied
End

ID	Step	Description	Involved
	Start/Creation and Prioritisation	Ticket has been determined to be a P4 or P3 incident as per the prioritisation workflow.	
1.	Assign Ticket to L2	Ticket has been Assigned to Level 2 after initial review in the DSS Triage workflow.	DSS Level 2 Support
2.	Confirm if Level 3 Assistance is required	Confirmation by Level 2 Support on if Level 3 assistance is required. If so, continue to step 3.	Level 2 Support
3.	Raise ticket in ServiceNow	Ticket raised by Level 2 Support to Level 3 Support for assistance.	Level 2 Support Level 3 Support
4.	L2 Technician/L3 Team assigned	Level 2 Support/Level 3 Support assigned to the ticket to investigate.	Level 2 Support Level 3 Support
5.	Investigation progressing or no progress	Level 2/Level 3 Support to investigate and find a fix. Jira ticket is updated if there is any notable progress.	Level 2 Support Level 3 Support
6.	Fix Applied	Level 2/Level 3 Support believed fix has been found and has resolved the issue.	Level 2 Support Level 3 Support
7.	Confirm fix with business.	Level 2 Support to contact stakeholders and see if the issue has been resolved on their end. If issue is not resolved, go back to 5 and reinvestigate issue.	Level 2 Support End User
8.	Close Jira Ticket	Jira ticket to be closed once it has been confirmed that the incident is resolved. Communications will be sent to the end user to advise.	Level 2 Support End User
	End		

Incident Lifecycle – High Priority (P2) Incidents


High Priority (P2) Incidents
Level 1&2 Support - DSD
Level 2 Support - DSD
Level 3 Support – DDS, NTT
DSD Incident Manager
Level 3 Support NTT
Level 2 Support DSD
Level 3 Support DDTS
Start
Creation and Prioritisation
1. Communications established
2. Handover to L2
11a. Comms update
15. Final release of comms
3. Are public comms required?
4. Statuspage alert created
5. Email comms drafted by L2
5a. Comms approved and Sent
6. Investigation begins
7. L3 assistance required?
8. Ticket generated in ServiceNow
9. Escalation request to L3 Incident Management
11. Investigation progressing or no progress
12. Fix applied
13. Confirm fix with business
14. Close Jira ticket
Incident Report Process
10. Ticket handed over to L3
11. Investigation progressing or no progress
12. Fix applied
End

ID	Step	Description	Involved
	Start/Creation and Prioritisation	Ticket has been determined to be a P2 incident as per the prioritisation workflow.	
1.	Communications established	Opsgenie alert and Teams chatrooms created.	DSD Incident Manager
2.	Handover to L2	Incident Manager hands over the incident advising the priority of the incident. L2 support to designate a team member as the Incident Owner for the duration of the incident.	DSD Incident Manager Incident Owner Level 2 Support
3.	Are public comms required?	Based on scale and the perceived impact, Incident Owner is to determine whether email communications and Statuspage alerts are required. If they're required, continue onto step 4. If not, skip to step 6.	DSD Incident Manager Incident Owner
4.	Statuspage alert created	The Incident Manager will create a Statuspage alert advising of outage.	DSD Incident Manager
5.	Email comms drafted by L2	The Incident owner (or anyone in the L2 Support team that's available) will draft all-staff email and send it for review and approval.	Incident Owner Level 2 Support
5a.	Comms approved and sent	Once the all-staff email has been approved it will be provided to the Incident Manager to send out. The Incident Manager will do a quick review to ensure the email is formatted neatly and in-line with standard comms.	Incident Owner DSD Incident Manager
6.	Investigation begins	L2 will begin their investigation of the incident. This may include reviewing logs and past incidents to find a previously used resolution.	Incident Owner Level 2 Support
7.	L3 assistance required?	The Incident Owner will determine whether the incident needs to be escalated to NTT or DDTS for further assistance. If escalation is required, continue to step 8. If escalation is not required, continue to step 11.	Incident Owner DSD Incident Manager
8.	Ticket generated in ServiceNow	The Incident Owner will create a ticket in the relevant ServiceNow instance in preparation of receiving DDTS or NTT assistance. This ticket number will be added into the comments of the Jira ticket.	Incident Owner
9.	Escalation request to L3 Incident Management	The Incident Manager will request the ServiceNow number, and a brief description of the resource required from the Incident Owner.	DSD Incident Manager Level 3 Incident Management Incident Owner

		The Incident Manager will then request an escalation for resource with the relevant Level 3 Incident Management team, providing them the ticket number and description of resource.	
10.	Ticket handed over to L3	Level 3 Incident Management will relay the information across to the relevant L3 support team and request their assistance in resolving the incident.	Level 3 Incident Management Level 3 Support
11.	Investigation progressing or no progress	L2/L3 will work on the incident and attempt fixes or workarounds to resolve the issue. If there is any major progress, then an update to communications may be required.	Level 2 Support Level 3 Support
11a.	Comms update	An update to go out via relevant communication channels when required. If there's no specific updates, then a general update will be released via Opsgenie and Statuspage.	DSD Incident Manager Incident Owner
12.	Fix applied	L2/L3 have found a potential fix for the issue and have implemented it. If a change is required to implement a fix, then Change Management processes will follow.	Level 2 Support Level 3 Support
13.	Confirm fix with business	L2/L3 will confirm with the business whether the fix has resolved the issue or not. If the issue is persisting, then return to step 11. If the issue has been fixed, continue to 14.	Level 2 Support Level 3 Support End User
14.	Close Jira ticket	Closure notes to be added to the Jira ticket advising of what resolved the incident. Ticket will then be marked as resolved and then marked as closed to ensure it does not reopen.	Level 2 Support Level 3 Support Incident Manager
15.	Final release of comms	Final update for Statuspage and Opsgenie advising of closure of incident. If email communications were released, a resolution email will be released to all-staff.	Incident Manager Incident Owner
	End		

Incident Lifecycle - Major (P1) Incidents

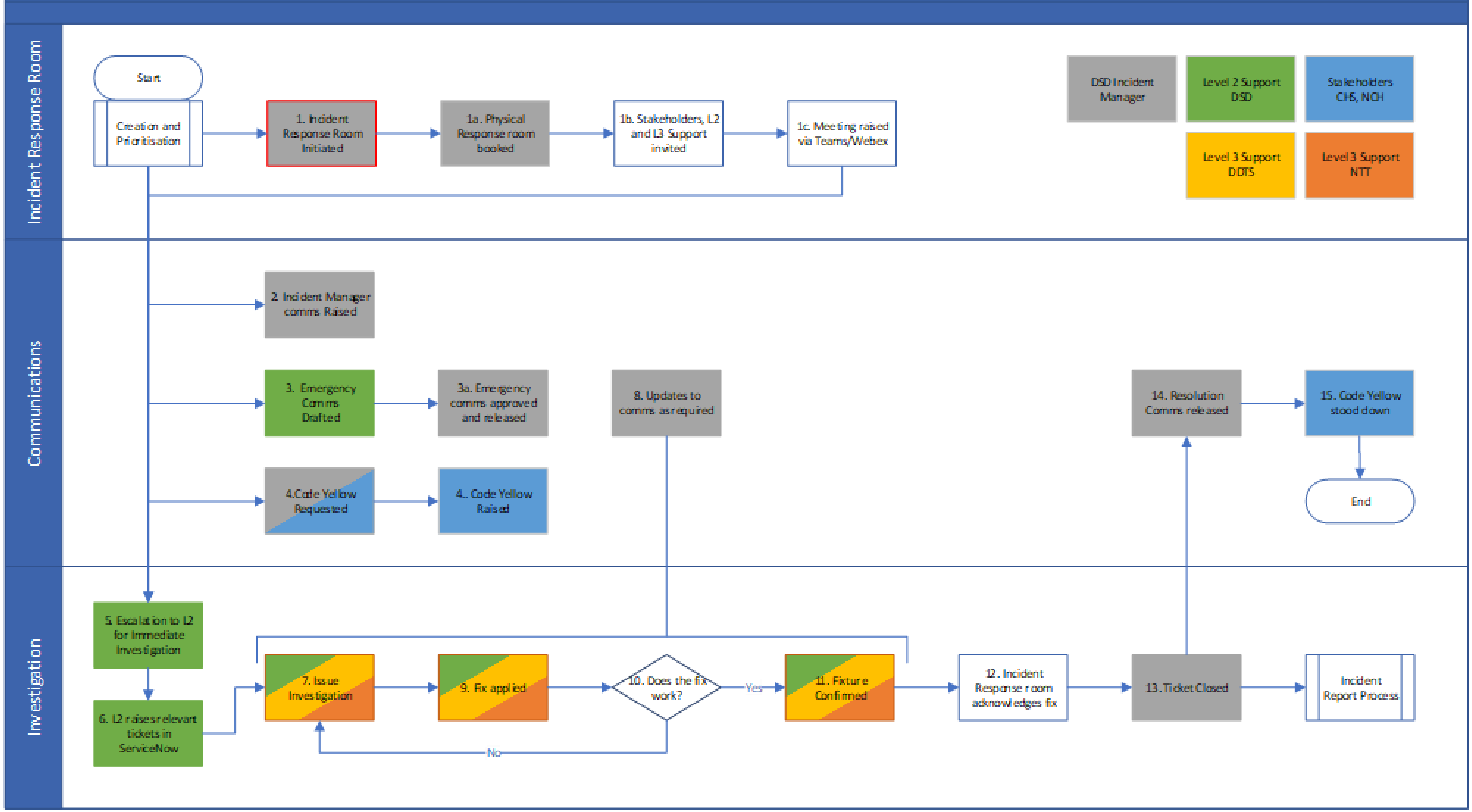
A major incident is the highest category of impact for an incident. A major incident results in significant disruption to the ACT Government business affecting an organisation's ability to continue service provision.

In the event that considerable impact to or loss of ICT Services is identified, the incident is immediately escalated to the Major Incident Management Team for determination on how the incident will be managed. One or more of the following officers will determine if the incident is to be managed as a major incident requiring the formation of the Major Incident Management Team:

1. DSD Incident Manager; if unavailable
2. IT Service Management Director; if unavailable
3. Senior Director, Software, Architecture and Support Hub; if unavailable
4. Digital Solutions Division Executive.

Upon the determination that the incident is Major, the DSD Incident Manager will activate the Incident Response Room.

Major (P1) Incidents


Incident Response Room
Communications
Investigation
Start
Creation and Prioritisation
1. Incident Response Room Initiated
1a. Physical Response room booked
1b. Stakeholders, L2 and L3 Support invited
1c. Meeting raised via Teams/Webex
DSD Incident Manager
Level 2 Support DSD
Stakeholders CHS, NCH
Level 3 Support DDTS
Level 3 Support NTT
2. Incident Manager comms Raised
3. Emergency Comms Drafted
3a. Emergency comms approved and released
8. Updates to comms as required
14. Resolution Comms released
15. Code Yellow stood down
End
4.Code Yellow Requested
4.. Code Yellow Raised
5. Escalation to L2 for Immediate Investigation
6. L2 raises relevant tickets in ServiceNow
7. Issue Investigation
9. Fix applied
10. Does the fix work?
Yes
No
11. Fixture Confirmed
12. Incident Response room acknowledges fix
13. Ticket Closed
Incident Report Process

ID	Step	Description	Involved
	Start/Creation and Prioritisation	Ticket has been determined to be a P1 incident as per the prioritisation workflow.	
1.	Incident Response Room initiated	This is to be done in parallel with steps 5 and onwards. Incident Manager determines that incident is a P1 and begins protocol for standing up the Incident Response Room.	DSD Incident Manager
1a.	Physical response room booked	There are two locations in Bowes street that can house the physical venue for the response room. These locations are either 4.04 (The teleconference room) or the DSOC Incident Response Room on ground floor. The Incident Manager will book one of the two locations for the duration of the outage. At the same time, any stakeholder that cannot come to Bowes will make necessary measures to book meeting rooms at TCH or NCH.	DSD Incident Manager Stakeholders
1b.	Stakeholders, L2 and L3 support invited	The Incident Manager will created a meeting invitation and forward it to all relevant stakeholders, directors/senior directors, and Level 3 Incident Management members. This meeting invite will either be for Webex or MS Teams.	DSD Incident Manager Stakeholders Level 2 Support Level 3 Support Incident Management
1c.	Meeting raised via Teams/Webex	The meeting starts and is accessible either via Webex or MS Teams. All relevant parties will join for the duration of the incident to provide and receive updates in real-time.	DSD Incident Manager Stakeholders Level 2 Support Level 3 Support Incident Management
2	Incident Manager comms raised	Opsgenie and Statuspage alerts are raised for the incident.	DSD Incident Manager
3	Emergency Comms drafted	Incident owner to draft all staff email comms. Comms will be reviewed at the Incident Response Room to ensure they're fit for sending. It would also be suggested to call out in the comms for staff to initiate Business Continuity Processes.	Incident Owner Stakeholders DSD Incident Manager
3a.	Emergency comms approved and released	Once approved, Incident Manager will release the email to all staff.	DSD Incident Manager

4	Code Yellow Requested	A request for a Code Yellow alert to be raised may be requested by either Incident Manager or stakeholders.	DSD Incident Manager Stakeholders
4a.	Code Yellow Raised	Code Yellow will be raised via CHS and NCH.	Stakeholders
5	Escalation to L2 for immediate investigation	While stages 1 through 4 are actioned, the Jira ticket will be sent to Level 2 for immediate escalation and resourcing. The Incident Owner will be determined here if one hasn't been chosen already.	Level 2 Support Incident Owner DSD Incident Manager
6	L2 raises relevant tickets in ServiceNow	L2 will create a ServiceNow ticket with either NTT or DDTS for assistance in the investigation of the incident. When a ticket is generated, the Incident Owner will provide it to the Incident Manager to share in the Incident Response room and to acquire L3 resource.	Incident Owner Level 2 Support DSD Incident Manager Level 3 Incident Management Team
7	Issue Investigation	Investigation of the incident begins. L2 and/or L3 will actively look for potential fixes to resolve the issue. Any updates on the status of the investigation may be provided from the Incident Owner to the Incident Response Room for awareness.	Level 2 Support Level 3 Support Incident Owner
8	Updates to Comms as required	This step can be completed at any time during steps 7 through 11. Updated communications released through any of the released methods (email, Statuspage, Opsgenie or Code Yellow alerts).	DSD Incident Manager
9	Fix Applied	A fix has been found and applied for testing. A fix may be subject to Change Management procedures depending on the type of fix applied. If this is the case, then the Incident Owner will be required to create an emergency change.	Level 2 Support Level 3 Support Incident Owner
10	Does the fix work?	L2/L3 will liaise with a few affected users to determine if the fix has worked. Additionally, reports of the effectivity of the fix may be received through the stakeholders in the Incident Response Room. If the fix has not resolved the incident, go back to step 7. If the fix has worked, proceed to step 11.	Incident Owner Level 2 Support Level 3 Support Stakeholders
11	Fixture confirmed	Fix has been confirmed and issue has been resolved. If a change had not been created during step 9, then one may be created now that the issue has been resolved. Monitoring may occur during this step to ensure that the fix applied isn't temporary.	Incident Owner Level 2 Support Level 3 Support

12	Incident Response room acknowledges fix	Incident Owner reports findings from the fix to the Incident Response Room. The members of the meeting will then discuss and accept whether they accept the results of the fix.	Incident Owner DSD Incident Manager Stakeholders
13	Ticket Closed	Ticket is marked as resolved and then closed, noting the duration of the outage in the ticket. At this stage the Incident Response Room may be stood down and relevant members may begin to return to BAU activities.	Incident Owner DSD Incident Manager
14	Resolution Comms released	Closure and resolution communications released on all comms channels that went out. Comms will advise staff to stand down Business Continuity Processes and return to BAU activities.	DSD Incident Manager Incident Owner
15	Code Yellow stood down	The call to stand down the Code Yellow is made by CHS/NCH stakeholders.	Stakeholders
	End		

Records Management

Records must be managed in accordance with the Territory Records Act 2002 and ACTHD policy and procedures.

Post Incident Reports

A Post Incident Report (PIR) is created as a result of a P1 or P2 incident. The PIR is a record of what had happened and what the goals are to ensure that it doesn't happen again. A PIR is initiated by the Incident Manager who fills out the basic details of the incident, then sending it to the Incident Owner for the technical additions.

The PIR is split into two sections: the front page and report details.

The front page is partially generated on export, taking various pieces of information which have been recorded in the Jira incident ticket case notes. The PIR contains information on the ticket numbers, who the incident owner is, whether there has been engagement with the Incident Manager, and times raised and resolved. It also includes the system name, criticality, and impacted hours.

The following pages of the Post Incident Report cover at a high level the cause and findings of the incident. Below will advise what each section is and what is expected to be written in the report:

Business Impact

The Business Impact will detail the direct impact the outage has had on the Health Directorate as a whole. This section will advise on what systems are affected if there is any upstream or downstream impact, users affected and potential impact on patient care if any.

Incident History

This section details a high-level background of the Incident. If there is a prior history of similar outages, then they are to be outlined first. Once previous outages are outlined, specifics of this Incident may be listed.

Incident Timeline

This section should detail every major update for the incident from the start of the ticket being raised until the closure and confirmation of resolution. Any meaningful encounters and updates that happened within the ticket. This area should be supplemented with any notes that had put into the Opsgenie alert.

Linked Issues

This section is an optional one that is automatically generated if there are any linked tickets to the incident at the time of export. Its purpose is to compliment the business impact by showing how many related tickets were raised during the outage, if there were any.

Communications

This section details the communications that were both received and sent for the Incident. Explain whether the DSD Incident Manager was notified and if there were any communications between DSD and the vendor. Opsgenie alerts and email communications to clients are also to be listed here.

Technical Troubleshooting

This section is for presenting the technical findings of the incident. Even if a root cause is not found, the technical fix should be detailed with the potential cause.

Root Cause

If a root cause has been found for the incident, then this section explains what that cause is and any background around it. This section may tie into Incident history if there has been any prior tickets that have already raised this. If there is no root cause found at the time of the report, then it is expected that any potential ideas are listed for review.

Recommendations

This is a self-assessment detailing what the Incident Owner and broader Level 2/Level 3 Support teams will do to ensure that resolution is permanent. If no root cause is found, then the recommendations should include what the plan is to find it and should also include any risk mitigation for the future.

Once the details of the report have been filled out, the Incident Owner's Senior Director will review and sign off on the release of the PIR. It will then be sent to the Incident Manager who will table it for the next Change Control Board and include any recommendations in the Recommendations Register.

Recommendations Register

The Recommendations Register is an excel spreadsheet that is kept internally by the Incident Manager. This register contains all recommendations that have been made in response to a P1 or P2 incident on whether they have been actioned or not.

The Incident Manager will send a report out to all Senior Directors monthly to request an update on whether a recommendation has been actioned or not. If they can't be actioned for whatever reason, then they will be marked as cancelled and the reasons noted in the register.

Implementation

The AHD Incident Management Procedure will be published on the Health HQ policy and procedure register.

The Incident Manager will incorporate the content into an incident management training plan which will consist of targeted in-service training for all identified roles within the procedure.

The procedure will be used to develop knowledge base articles and used as a source of reference for ongoing training for the organisation.

References and Related Documents

Below you can find a list of references, websites, and knowledge articles that this document references or that reference this document.

References

- Information Technology Infrastructure Library v4 Framework
- DDTS Incident Management Policy article
- Health Emergency Plans
- Atlassian - Incident Communication
- Atlassian - Incident Response Best Practices

Legislation

- No Applicable Legislations

Supporting Documents

KB Articles referencing this Procedure:

- Incident Management – Business Hours Incident Process
- Incident Management – How to add notes to an Opsgenie Alert
- Incident Management – Out of Hours Process
- Incident Management – Post Incident Report Guide
- Incident Management - Recommendations page

Version Control

Version	Date	Comments
1.1	13/07/2023	• General updates ○ Removal of Calvary/Addition of NCH • Removal of day/night shifts • Slight adjustments to the Post Incident Report section • Communications update ○ Addition of Statuspage, Technical and Executive Teams chats, Health IM Teams channel, SMS Dashboard ○ Creation of General incident email templates • RACI updates • Full review and update to workflows
1.0	12/09/2022	Approved by Chief Information Officer.

Disclaimer: *This document has been developed by the ACT Health Directorate specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and the ACT Health Directorate assumes no responsibility whatsoever*

Appendix A – Government Critical Systems

Please note that all the systems in this list are currently Active or Read-only.
Systems that have been retired and/or decommissioned have been removed from this list.

Jira Assets System Name	DDTS CMDB System Name	Common Name
AccessControl	AccessControl	Access Control
ACTPAS	ACTPAS	ACTPAS
ACTPAS-REPORTING	ACTPAS-REP	ACTPAS Reporting
AustcoTaceraNurseCall	AustcoTaceraNurseCall	Nurse Call
Avigilon	Avigilon	Avigilon
BMS-NETWORK	BMS-NETWORK	Building Management System
CCURE	CCure	Ccure
CLINICALPORTAL	CLINICALPORTAL	Clinical Portal
CLINICALWORKDEVICES - Android	CLINICALWORKDEVICES	Clinical Work Devices
CPF	CPF	Clinical Patient Folder
DATAHEALTH	DATAHEALTH	Data Health
DHR	DHR	Digital Health record
Duress - Ascom	ASCOMDURESS	Duress
DURESSALARM	-	Duress
EDIS	EDIS	EDIS
EMM	EMM	EMM Medchart
Health Enclave	HealthEnclave	Health Enclave
JACQUES	-	Jacques
KESTRAL-PLS	KESTRAL-PLS	Kestral PLS
MERLIN	MERLIN	Merlin
MerlinMap	MerlinMap	MerlinMap
METAVISION	METAVISION	Metavision
Mobile Device Manager - SOTI	SOTI	SOTI
Mobile Duress - IQ Messenger	MobileDuress-IQM-HealthEnclave	IQ Messenger
Notifiable Disease Management System	Notifiable Disease Management System	NDMS
NURSE-CALL	NURSE-CALL	Nurse Call
OneHealth	OneHealth	One Health
PEGACORN	PEGACORN	Pegacorn
SPOK	CRITICALCOMMUNICATIONS	SPOK
Territory Radio Network	TRN	TRN
Traka	Traka	Traka
Zello	Zello	Zello

Table 5 – Government Critical Systems, taken from both Jira Insight and ServiceNow

Appendix B – OpsGenie Notification Examples

No.	Stage	Considerations	Messages that may align with this stage
1.1	Incident Identification	identification of an Incident.	No Opsgenie notes.
1.2	Logging and Incident	Raising of the incident.	No Opsgenie notes.
2.1	Escalating an Incident to Level 2 Support	Initial raising of the Ops-genie alert here.	• Incident reported. L2 technicians investigating. • L2 technicians triaging.
2.2	Investigation and Diagnosis	Issue being diagnosed and investigated. Also the period where a ticket will be raised to vendor for assistance if needed.	• Cause found. L2 investigating fix. • Incident escalated with L3. Awaiting response. • Incident raised with vendor. Awaiting response from vendor. • Incident raised with vendor. • Incident escalated to L3. Incident number X • L3 found cause. Technicians investigating fix. • Investigation ongoing by L3 technicians. • Investigation ongoing by vendor.
2.3	Escalation to Incident Management		• Escalation request sent for Incident Management approval. • Incident Manager escalated incident to L3.
3.1	Resolution	Fix has been applied, tested, and confirmed or denied.	• Fix applied. L2 technicians testing and confirming resolution. • Fix applied. L3 technicians testing and confirming resolution. • Fix applied. Vendor testing and confirming resolution. • Fix has not resolved the issue. L3 investigating. • Fix has not resolved the issue. L2 investigating.
3.2	Incident Closure		• Confirmed fix has resolved issue. Closing Incident.
3.3	Post Incident Actions		No Opsgenie notes.

Table 6 – Opsgenie Notification Examples