Major Incident Procedure

This reference guide summarizes the Major Incident procedure and is intended to assist Major Incident Managers (MIMs) in ensuring a timely and efficient resolution of Major incidents.

McGill University

MIM Quick Reference Guide

9/5/2013

A Reference Guide for MIMs

Contents

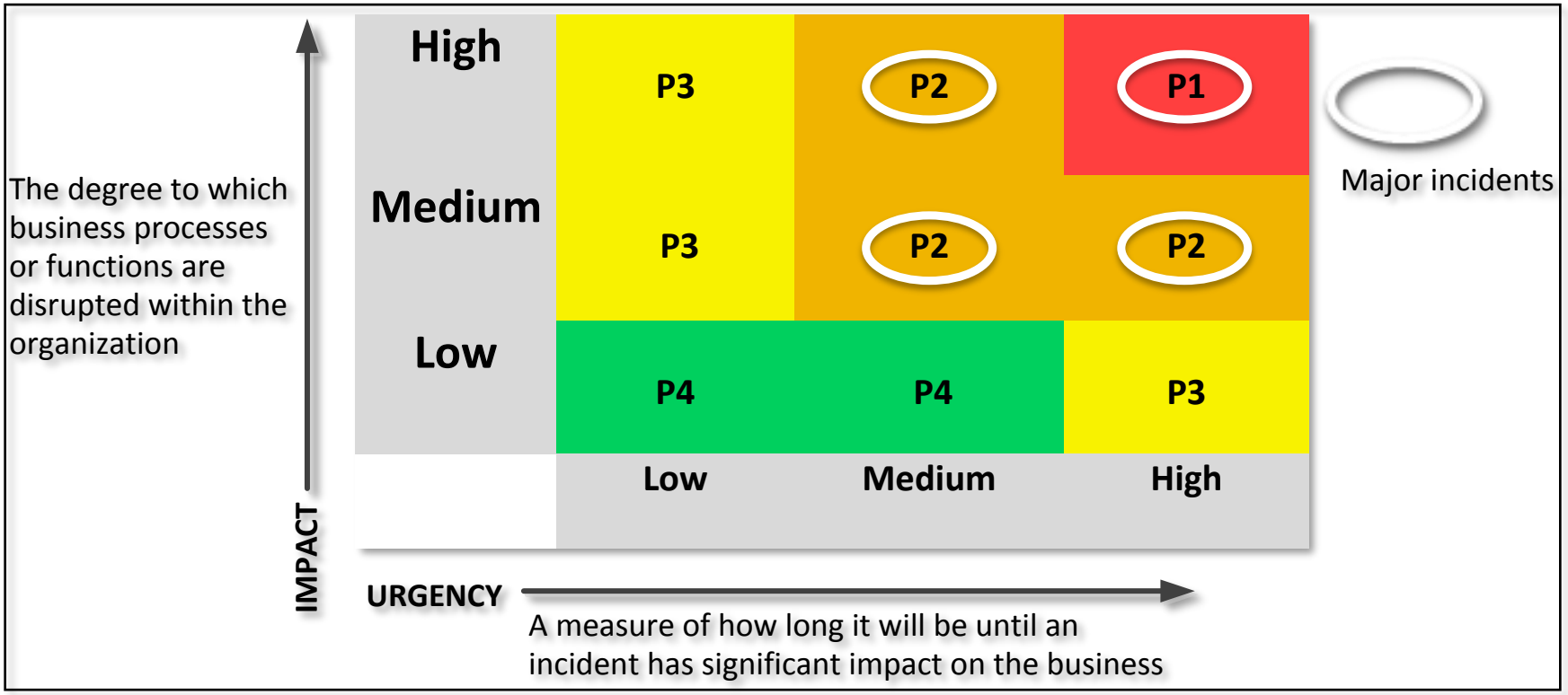
Related Policies

- An incident is categorized by the service appearing in the customer-facing IT Service Catalog.
- An incident is prioritized by assessing urgency and impact. Any change to the priority is negotiated and communicated to the business.
- A ticket has to be opened for each incident prior to the start of any work on the incident. If the Service Desk does not open the ticket, the Tier 2-N Incident Resolver is responsible for ensuring that the Service Desk is aware of the ticket.
- Major Incidents are managed through a separate procedure that requires the nomination of a single manager for the incident from a pool of management staff in McGill IT Services. For security-related Incidents, Information Security assigns resources.
- The Major Incident Notifications Coordinator is responsible for the communication of all Major (P1/P2) Incidents to the business.
- The Service Desk owns all tickets throughout their lifecycle. The Service Desk is responsible for tracking progress, keeping users informed and closing the ticket.
- The business confirms that service has been restored (to an agreeable level of service), before any business-impacting incident ticket is closed.
- Any proposed activity to restore a service that potentially impacts other services is approved by the respective Service Owner.
- Any proposed service restoration for an incident that necessitates a change follows the McGill Change Management Process.

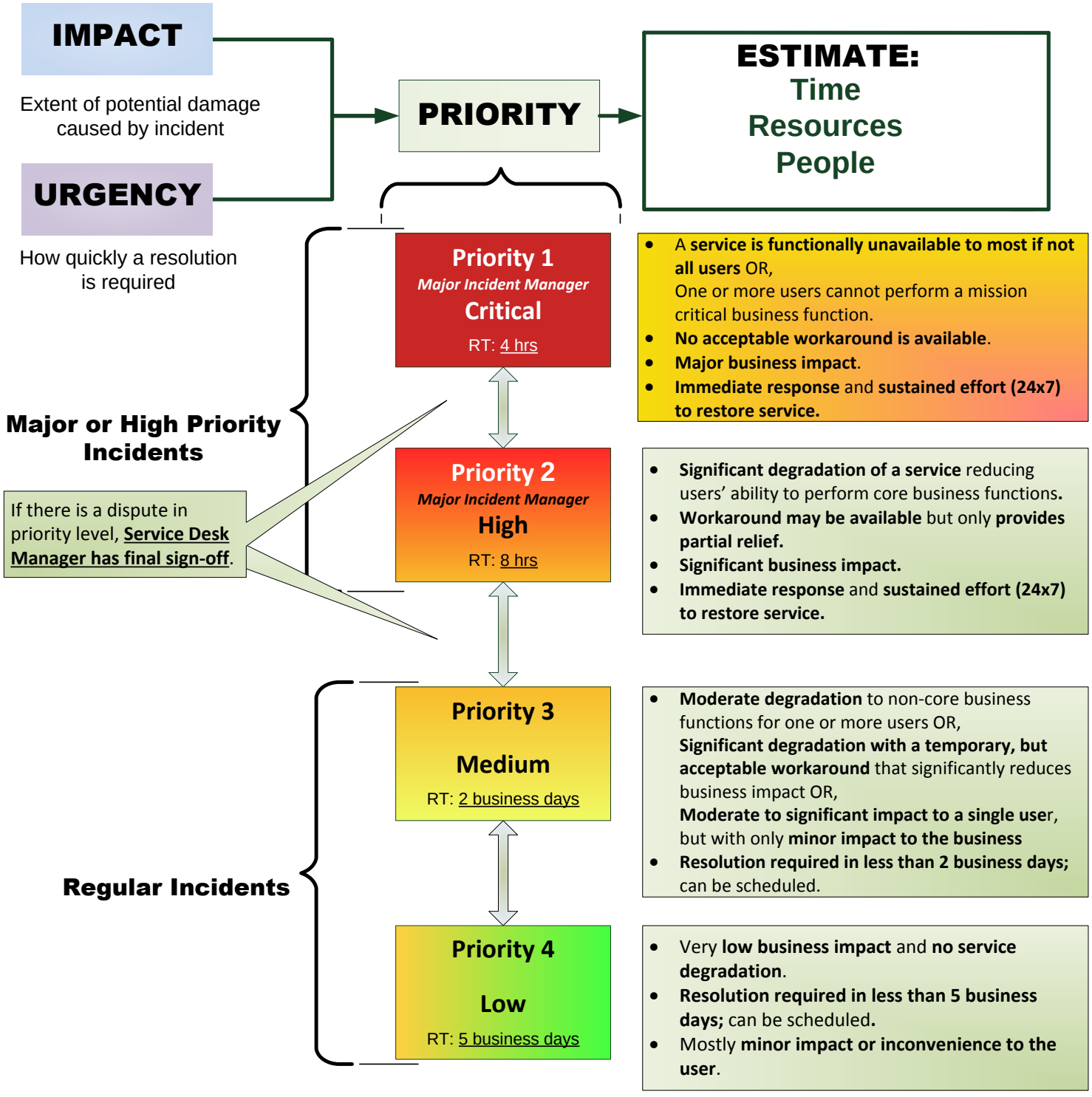
Source: McGill ITS Incident Management Process Guide v1.0

Priority Table

To be considered a **Major Incident**, an incident must be classified as **High** or **Medium Impact** and **High** or **Medium Urgency**.

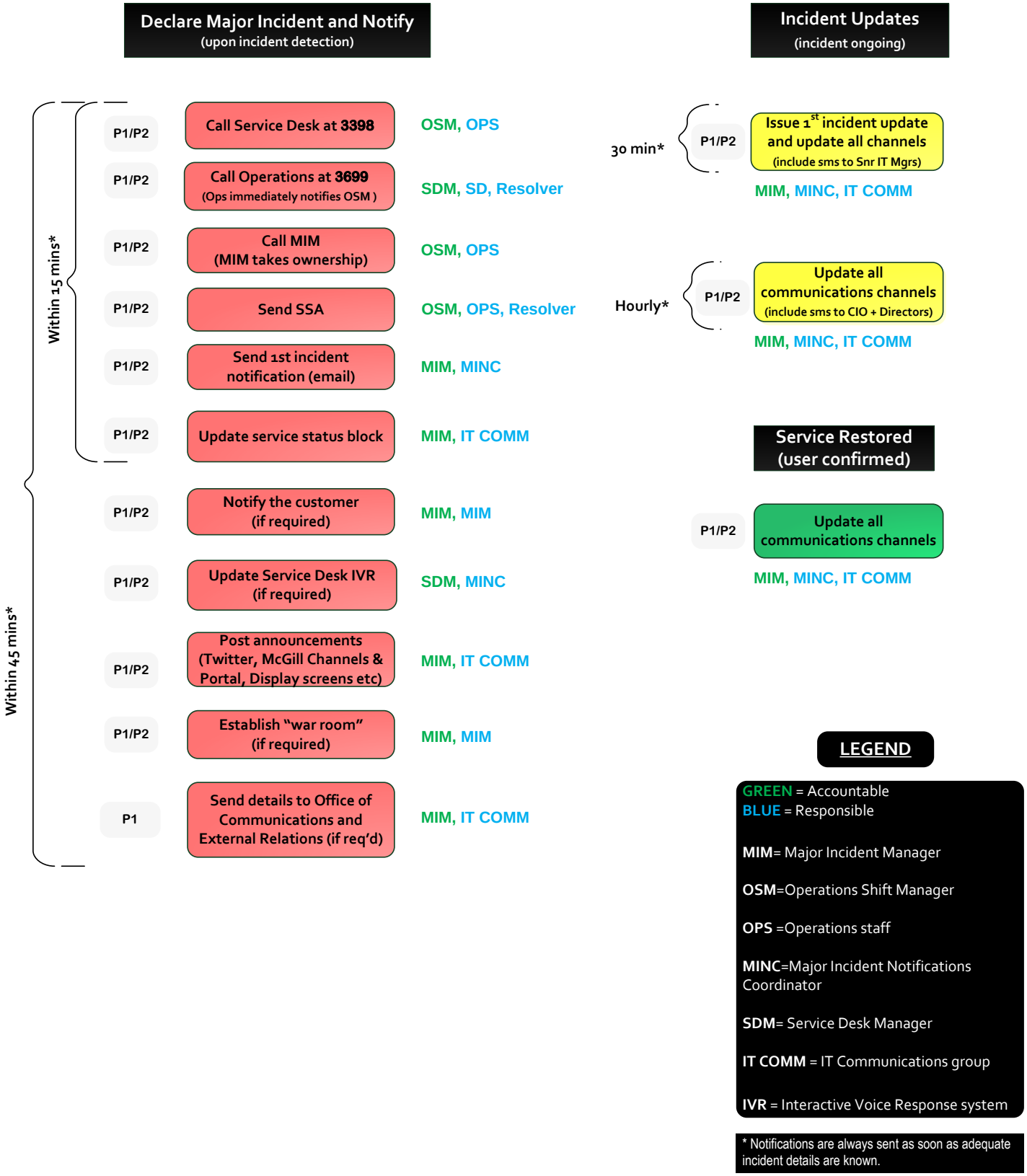


Incident Prioritization



LEGEND:
RT = Resolution Target

P1/P2 incident notifications (Mon to Fri 8 am – 5 pm)



LEGEND

GREEN = Accountable
BLUE = Responsible

MIM= Major Incident Manager

OSM=Operations Shift Manager

OPS =Operations staff

MINC=Major Incident Notifications Coordinator

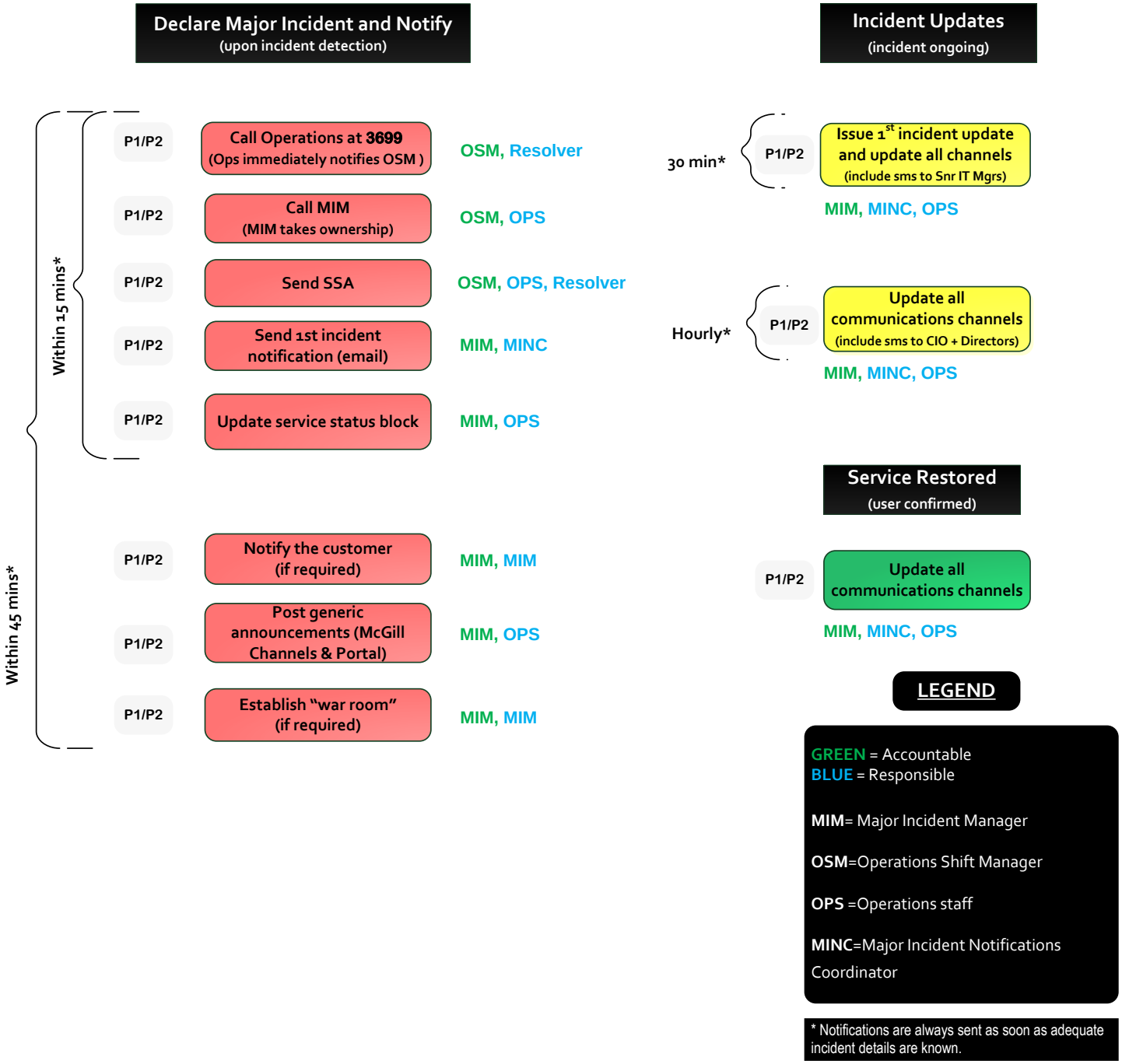
SDM= Service Desk Manager

IT COMM = IT Communications group

IVR = Interactive Voice Response system

* Notifications are always sent as soon as adequate incident details are known.

P1/P2 incident notifications (Mon to Fri 8 am – 5 pm)



Checklist of Tasks and Responsibilities

SITUATIONAL ASSESSMENT (OSM)
☐ What is the **Impact** of the incident on business processes and functions?
☐ How long will the incident take (**Urgency**) to affect business operations?
☐ Is there a suitable continuity or recovery plan available within the first 30 minutes?
☐ Is the service recovery effort highly complex?
☐ Does the incident affect several critical business services?
☐ Does the recovery of the service require the coordination of a large incident resolution team?
☐ Is this likely going to be a prolonged incident?

INITIAL RESPONSE TASKS (Operations/Service Desk)

☐ Inform Operations at 514-398-3699

☐ Create an incident ticket and assign priority 1 or 2

☐ Send a user-friendly notification through SSA

☐ Escalate to the Operations Shift Manager (OSM)

MAJOR INCIDENT MANAGER INCIDENT RESPONSE

1. Establish Command

☐ Take ownership of the incident and acknowledge ticket assignment
☐ Establish link with MINC
☐ Establish Major Incident team
☐ Choose and establish a "war room"

2. Establish Plan

☐ Convene kickoff meeting (if required)
☐ Review known facts (what do we know about the incident?)
☐ Develop systematic plan of attack (how do we want to restore the service, do we have a recovery/continuity plan?)
☐ Determine if vendor services are required
☐ Establish and agree on schedule for team meetings and escalations
☐ Send status report to MINC and keep a log of events

3. Execute Plan

☐ Ensure Resolvers conduct diagnostic activities to restore the service
☐ Approve identified workaround / solution
☐ Submit a Change request (RFC)

4. Manage Plan

☐ Conduct planned review meetings
☐ Manage functional and hierarchical escalations
☐ Send periodic updates to MINC
☐ Engage Problem Management if root cause analysis is needed to restore the service

5. Manage resolution

☐ Notify Service Owner of resolution plan
☐ Ensure fix or workaround is tested and executed to restore the service
☐ Ensure all steps taken to restore service are documented in a ticket
☐ Ensure all ticket assignments are completed; re-assign the incident ticket to Service Desk

6. Manage Post incident activities

☐ Close out logs and complete Preliminary Incident Report
☐ Schedule a Major Incident review
☐ Prepare and distribute the Final Incident Report

Incident Status Report

The Major Incident Manager must issue a status report to the MINC as soon as the incident is declared Major, and release status updates periodically until the incident is resolved.

Incident Ticket number:	
Prepared by:	

Current Situation

What has happened, which service (s) is affected, business impact and an updated forecast of when normal service will be restored.

Plan to restore service

What is being done to restore normal service? What are the anticipated activities and priorities within the next hour?

Comments

Is there any advice or workaround to aid users impacted by the incident?

Major Incident Report

The Major Incident Manager must issue a final report after the incident has been resolved.

Incident Ticket number		**Prepared by**	
Time ticket created	Enter date, time.		
Report Date	Enter date, time.	**Priority**	Choose the Priority.

Incident subject			
Service (s) impacted			
Incident start time	Enter date, time.	**Reported by**	
Incident detection time	Enter date, time.		
Date and time Service was restored	Enter date, time.	**Incident duration**	
Incident ticket status	Choose a ticket status.	**Related RFC (if any)**	
Incident Root Cause (if known)			
Root Cause Category	Choose a category.		
Incident Summary	Provide a detailed summary of what happened		

Business Impact
Explain how and to what extent the business was affected.

Incident Chronology	
Date, Time	Provide a chronology of events from incident discovery to service restoration. Insert other rows if necessary. At the minimum, include the following: • Who first discovered the incident • Description of any major tasks undertaken throughout the incident • Who restored the service and how it was carried out

Workaround / Solution
Describe the workaround or permanent solution that was used**. If only a workaround was** provided**, please** describe **the plan for a permanent solution.**

Lessons Learned
1. What did not go according to plan; were there any deviations from the documented procedures? 2. Were the documented Incident Management procedures followed? Were they adequate? 3. What information was needed before it was provided? Were any steps or actions taken that might have slowed or hampered the recovery? 4. What should the staff and management do differently the next time a similar incident occurs?
Recommendations for technology or infrastructure improvements
Recommendations for process improvement

Major Incident Review Action Items	Assigned To:	Status

Major Incident Team

Identify the resources (personnel) involved in the activities that were carried out as part of the incident process.

Name	Role	Actions Taken