Shared ICT Services

SICTS Major Incident Process

Owner:	Ruth Hicks
Authorised By:	
Date:	09/02/2020
Version:	Draft 2
Document Location:	Link to Document

Shared ICT Services

Document Control

Effective as of	13/02/2020	**Review Date**	13/07/2020

Change Record

Date	Author	Version	Reason for Change
09/02/2020	Ruth Hicks	0.1	Draft
13/02/2020	Ruth Hicks	1.0	Production

Contributors

Name	Position	Date Reviewed

Approved by

Name	Position	Date

Related Documents

Document Name	Location
SICTS Major Incident Procedure	**Under Development**
SICTS Incident Review Template	https://lbdigitalservices.sharepoint.com/sites/servicedoc/smd/SICTS Incident Review Template.dotx

Shared ICT Services

Contents

Major Incident Process Objectives

This document sets out to define the process to be followed when responding to a major incident, looking to address the following requirements

- to provide an effective communication system across the organisation(s) during a major incident
- to ensure that an appropriate Incident Manager is in place to manage a major incident
- that there are in place appropriate arrangements to ensure that major incidents are notified promptly to appropriate management and technical groups, so that the appropriate resources are made available
- to conduct major incident investigations and to contribute to the organisation's knowledge of the causes of incidents
- to provide timely information about the causes of incidents and any relevant findings from investigations
- to conduct a review of each major incident once service has been restored and, in line with problem management, to look at root cause and options for a permanent solution to prevent the same major incident happening again

Scope

All Incidents that require to be dealt with at P1 or P0 will be managed through this process.
Any ticket raised as a P1 through the normal ticket logging process will be downgraded to a maximum of a P2 and where appropriate the issue will be managed through this Major Incident process.

Definition of a Major Incident

A major incident is defined as a fault resulting to a core service being unavailable or suffering performance degradation such that staff are not able to work; affecting all or a significant number of users of that service.

Major incident Management

Prioritization

A Major Incident effecting one organisation (a single borough or the LGA) will be given a P1.
A Major Incident effecting multiple organisations (more than one boroughs or the LGA and at least 1 borough) will be raised as a P0.

The Major Incident should remain a P0 or a P1 throughout its life cycle. On rare occasions, the Head of IT (or their delegated representative) in effected organisation(s) may give permission for the priority of the Major Incident to be downgraded to a P2.

However, if it is downgraded to a P2 during its life cycle steps must be put in place to ensure that it is elevated back to its P0 or P1 status after it is closed, to enable its correct inclusion on reports.

Major Incident Ticket

The Service Desk will raise a specific ticket against the Major Incident service indicating the organisation(s) effected. This will use a member of the Service Desk Management as the 'Customer' to enable access to the Major Incident Service.

This Major incident ticket will be assigned to the appointed Major Incident Manager and all tickets related to the incident will be linked to it and all technical ticket updates will be added to it.

Related Tickets

All tickets related to the Major Incident will be linked on Hornbill to the Major Incident ticket. All linked tickets will be set to a P3.

Roles and Responsibilities

Accountability

The accountability for the documentation and running of the Major Incident Process sits with the SICTS Support Manager.

Major Incident Manager

The incident Manger will normally be a Service Desk Team Lead based in the Wembley office who is able to be in direct contact to the technical teams. However, the Support Manager, a Service Desk Team Lead on another site or a Senior Technical Analyst may perform this role. They will responsible for

- Raising the major incident ticket against the major incident service.
- Management of the Major Incident Ticket

- Ensuring that all Service Desk Staff are aware of the major incident ticket number and the types of ticket that need to be linked to it, with briefing to set as a P3 priority at the time that it is linked
- Liaising with the technical lead
- Sending the comms throughout the lifecycle of an incident (or at delegating them to a specific suitable member of staff to continue them in their absence)

Service Desk

The Service Desk team is key to the identification of Major Incidents by spotting trends and patterns in the incoming tickets. The service desk will ensure that any tickets are related to the Major Incident Ticket

On-Site support teams

Where appropriate (especially during outages effecting email systems) the On-Site teams will be responsible for floor walking to communicate the fact that there is known issue and that it is being dealt with.

Technical Lead (Major Incident Owner)

The technical lead will normally be the Team Lead or their appointed deputy for the technical team carrying out the investigations and working to resolve the issue.
The Technical Lead will be responsible for

- Co-coordinating technical efforts to restore service
- Updating the major incident ticket log with technical updates
- Updating the major incident ticket log with impact statements (ie confirmation of boroughs effected, what systems/connectivity is effected)
- Preparation of the Major Incident report at the conclusion of the incident.

Infrastructure Manager

Will assume the Technical lead in the event that the Major Incident requires input from multiple teams. They will be responsible for working with the Incident Manager to provide comms details and setting up a major incident 'War Room' with representatives from all the required technical teams and the incident manager.

Problem Manager

Responsible for liaising with the technical team(s) and the Major Incident Manager to produce a major incident report; responsible for ensuring that a root cause has been identified and a problem is logged where appropriate to ensure no further re-occurrence.

Change Manager

May need to process any urgent chances necessary for incident resolution.

Communication Plan

There will be communication at regular intervals throughout the Major Incident ticket Life Cycle.

The Aim of the communication plan during the incident it to communicate, in a purely non-technical way, details about the issue and the impact that can expect to been seen by the users in the organisations.

Technical communication of what the cause of the issue is, server names etc will be only be communicated in the Major Incident Report after the conclusion of the incident.

WhatsApp

Immediate comms regarding the identification of a Major Incident via the WhatsApp group – SCITS Stakeholder Update, this should reach all required senior staff in all organisations. Further updates will be posted to this group but the comms through Hornbill will be given priority during the incident.

Floor Walking

At Brent Civic Centre, Smith Square, Laurence House and 160 Tooley Street, SICTS On-Site staff will (especially during an issue with email) floor walk ensuring that people know that there is an issue and that SICTS is dealing with the issue as a matter of priority.

Emails from Hornbill

When a P1 is raised on Hornbill, an email is sent automatically to SICTS staff to alert them to the ticket.

The emails sent from the Major Incident ticket use a distribution lists for each organisation, with the emails being sent to every organisation that is identified by the Major Incident ticket, as being affected.

The distribution lists are as follows
Brent: HornbillMIP1@brent.gov.uk
LGA: HornbillMIP1@local.gov.uk
Lewisham: HornbillMIP1@lewisham.gov.uk
Southwark: HornbillMIP1@Southwark.gov.uk

Once the Major Incident Ticket is logged, a first update will be sent out from Hornbill using a Red – 'system down' Header ASAP to alert people to the fact that we are aware of an issue.

A second Red update will be sent within an hour of the first with a more detailed but non-technical statement regarding the impact (signs and symptoms) that will potentially be seen by an individual user.

Subsequent red 'system down' messages will be sent at two hourly intervals unless a reasonable statement to the contrary has been published on previous comms. For example if SICTS have been given a time on-site of 4 hour's time for a third party engineer to carry out work that SICTS cannot do themselves and which is clearly the cause of the major incident, a next comms update window of 4.5 or 5 hours may be stated.

Once SICTS believe that the issue has been resolved, an Amber update will be sent. This indicates that we believe that the issue has been resolved but we are continuing to test and monitor, or that the system down situation has been restored to provide a degraded service and we are still working on the issue.

Once SICTS are confident that the Major Incident has been fully resolved and that all testing indicates that the system is stable then a green 'Major Incident Resolved' message will be sent.

Major Incident Report

The technical lead will prepare the Major Incident report with full technical details of the issue, its resolution and lessons learned using the template. The naming format will include the Major Incident ticket number.

The MIR will be circulated to any identified Key Stakeholders within 10 working days of the incident occurring, with an MIR review scheduled shortly after that.

The Infrastructure Manager is responsible for ensuring that the Major Incident review process is followed.