University of California
San Francisco

Information Technology and Service

MAJOR INCIDENT PROCESS

VERSION 1.3, REV. November 2, 2012

Document Version Control

Document Name		ITS Major Incident Process	
Version Number	**Issue Date**	**Prepared By**	**Reason for Change**
1.0	8/31/12	Terrie Coleman	Initial draft
1.1	9/5/12	Terrie Coleman	Updates based on meeting with John Chin and Rebecca Nguyen
1.2	10/22/12	Terrie Coleman	Updated process diagram at the request of John Chin, step 14. Corrected RACI Chart.
1.3	11/2/12	Terrie Coleman	Updated MI Check list to include IT-911 and Med Center conference numbers. Removed ITS from title of document. Defined Med Center's IT AOC.

Reviewers and Approvers

Name	Approval Date
Kevin Barney	10/22/12
John Chin	10/22/12
Rebecca Nguyen	10/22/12
Darlena Torres	10/22/12

Table of Contents

1. INTRODUCTION

The purpose of this document is to define the actions, communications and escalation steps that will used to manage a major incident.

The major incident process has 4 key phases; Detection of the major incident, Escalation to Priority 2, Escalation to Priority 1 and Closure. The major incident process can be abandoned at any point once resolution of the incident has been reached.

2. DEFINITIONS

Term	Definition
Major Incident	Any full or partial system outage.
Technician	Resource tasked with identifying and resolving incident. Also responsible for providing regular updates to the Service Desk Staff.
Incident Response Team	Technical team tasked with identifying and resolving incident.
Service Desk Agent	Point of coordination for all incoming incident information and outgoing communications.
Service Desk Manager	Primary point of contact within the Service Desk accountable for escalations and end user notification.
Incident Commander	Individual who is responsible for driving the major incident to closure. This role is typically held by the manager or designee of the affected system or infrastructure component or by the security manager in the event of a major incident involving a breach.
ITS Administrator On Call (AOC)	The ITS director on-call responsible for providing enterprise perspective into the issue and making sure key leadership staff are notified of the issue, if necessary.
IT Administrator On Call (AOC)	The Med Center's director on-call responsible for providing enterprise perspective into the issue and making sure key leadership staff are notified of the issue, if necessary.

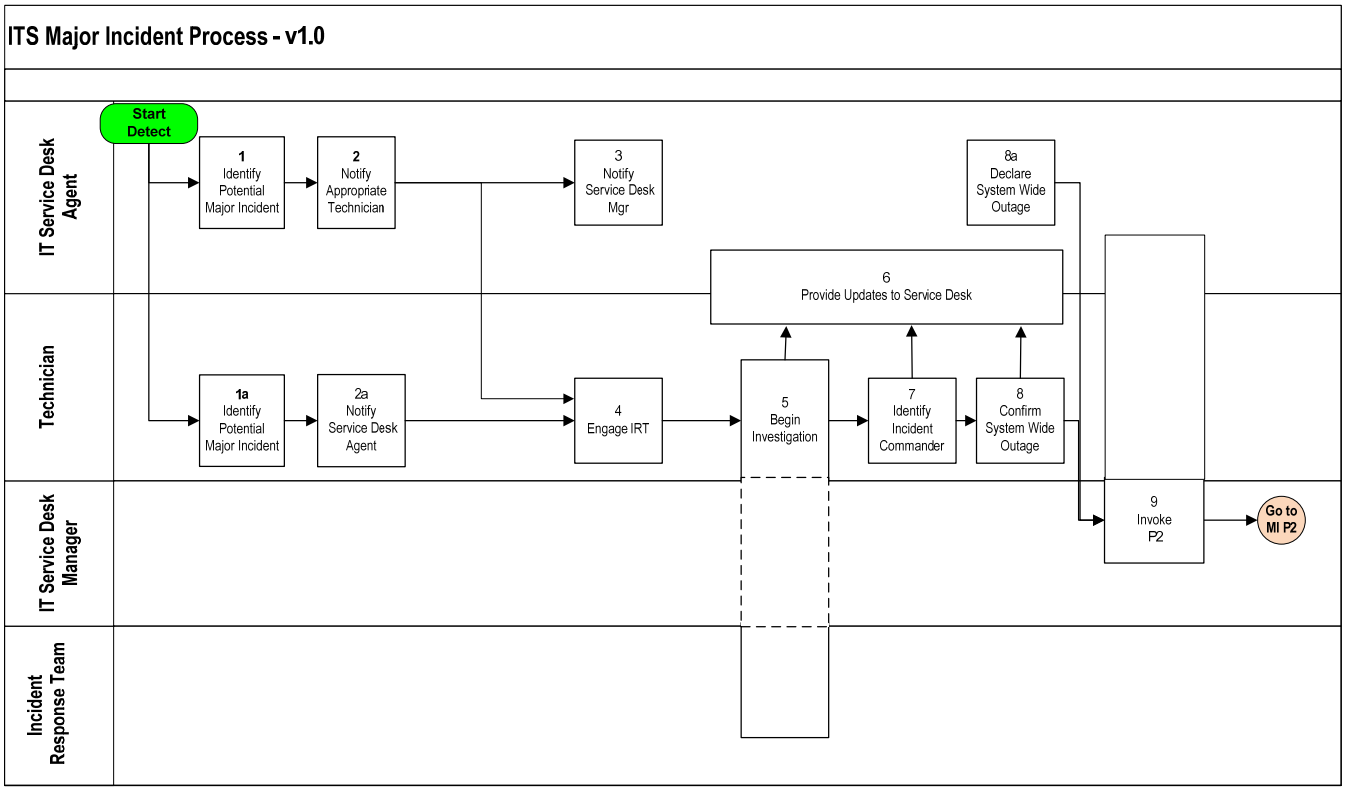
3. PROCESS DEFINITION

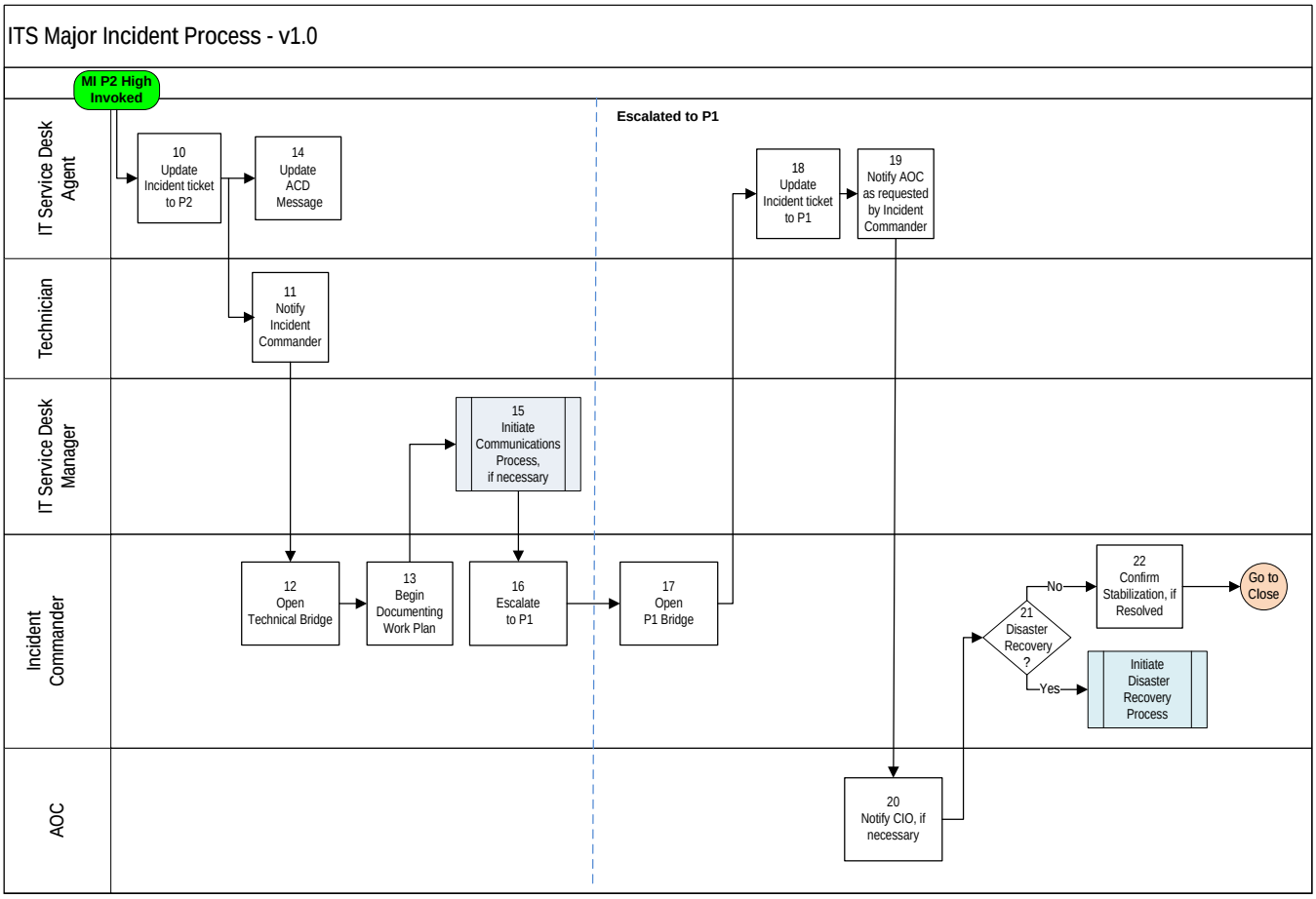
3.1. RACI CHART

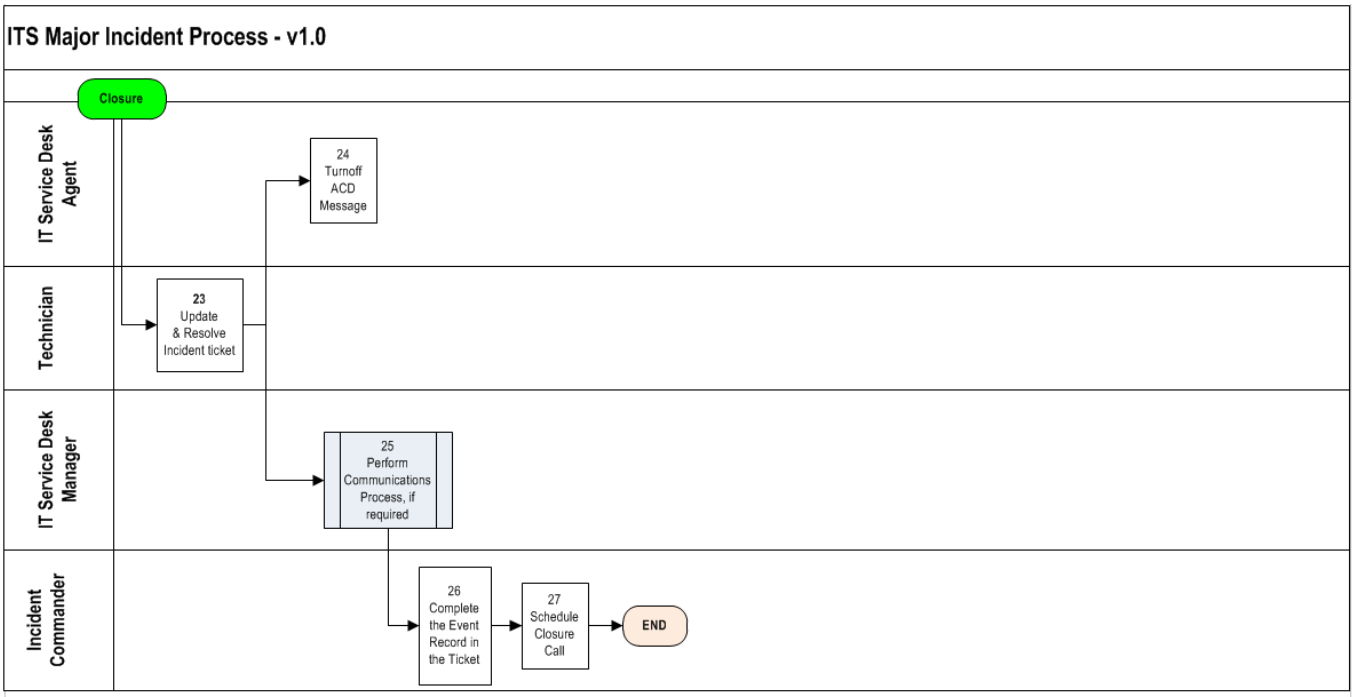
#	Major Incident RACI Chart	Technician	Service Desk Analyst	Service Desk Manager	Incident Commander	Incident Response Team	ITS AOC	CIO	Customer	Sys/Application Owner	Output	Notes
	Detection of Major Incident											
1	Identify Potential Major Incident (Pattern of issues reported to Service Desk)		A/R								Open Ticket	One of two possible starting points
2	Notify "On-Call" Technician and assign ticket	I	A/R								Assign Ticket	
1a	Identify Potential Major Incident (Monitoring tools)	A/R									Open & Assign Ticket	One of two possible starting points
2a	Notify IT Service Desk Potential MI	A/R	I									How to contact SD?
3	necessary	A/R				I						
4	Begin Investigation	A/R				R						
5	Provide SD with updates on Issue	A/R	I									
6	Identify potential Incident Commander	A/R	I	I	I							
7	Contact Service Desk Manager		A/R	I								
8	Confirm system-wide issue	A/R	C	C								
9	Invoke escalation to Major Incident P2	R	R	A/R	I							
	Escalation to P2 High											
10	Update IncidentTicket: Priority High (P2) Symptom to Major Outage	I	R	A	I	I					Automated Notification to ITS Mgers and Directors	
11	Notify Incident Commander	A/R			I						Continue Remediation	
12	Open Technical Bridge	I	I	I	A/R	I						
13	Begin documenting workplan - Event Record	C	I	I	A/R	C						
14	Update ACD message for inbound customers		R	A								
15	Initiate Communication Process, if required		R	A/R	R				I	I		
16	Escalate to Priority 1	C	I	C	A/R	C						
	Escalation to P1 Critical											
17	Open P1 ITS Bridge	I	I	I	A/R	I						
18	Update Incident Ticket: Priority Critical (P1) Symptom to Major Outage	I	R	A	I	I					Automated Notification to ITS Mgers and Directors	
19	Notify ITS AOC and relevant IT Teams as requested by Incident Commander		R		A		I					
20	Decision: Formal Notification to CIO?						A/R	I				
21	Decision: Cut over to Diaster Recovery, if available	I	I	I	A/R	I	C	C			DR or Continue Remediation	
22	Confirm Stabilization or Resolutions, if resolved	R	R	I	A/R	R	I	I			Issue Resolved	
	Closure											
23	Update and Resolve Incident Ticket	A/R	I	I	I	I	I	I			Automated Notification to ITS Mgers and Directors	
24	Remove Front-end ACD message		R	A								
25	Initiate Communication Process, if required		R	A/R	R				I	I		
26	Complete Event Record on ticket as necessary	C	I	I	A/R	C						
27	Schedule Closure Call	I	I	I	A/R	I	I	I				

Responsible – People who do the work, facilitate it and/or organize it
Accountable – The one who ensures that desired outcomes are reached and has yes/no decision making authority
Consulted – People who have critical expertise to contribute before a decision is made
Informed – People who are significantly affected by the activity/decision and must be informed to ensure successful implementation

3.2. ACTIVITY DIAGRAMS




ITS Major Incident Process - v1.0
MI P2 High Invoked
Escalated to P1
IT Service Desk Agent
Technician
IT Service Desk Manager
Incident Commander
AOC
10 Update Incident ticket to P2
14 Update ACD Message
11 Notify Incident Commander
15 Initiate Communications Process, if necessary
12 Open Technical Bridge
13 Begin Documenting Work Plan
16 Escalate to P1
17 Open P1 Bridge
18 Update Incident ticket to P1
19 Notify AOC as requested by Incident Commander
20 Notify CIO, if necessary
21 Disaster Recovery ?
No
Yes
22 Confirm Stabilization, if Resolved
Go to Close
Initiate Disaster Recovery Process


ITS Major Incident Process - v1.0
Closure
IT Service Desk Agent
Technician
IT Service Desk Manager
Incident Commander
24 Turnoff ACD Message
23 Update & Resolve Incident ticket
25 Perform Communications Process, if required
26 Complete the Event Record in the Ticket
27 Schedule Closure Call
END

4. APPENDIX

4.1. MAJOR INCIDENT CHECKLIST

ITS Major Incident Action Check List			
ID	**Detection of Major Incident (MI)**	**Action by:**	**Notes**
1	**Identify a Potential Major Incident** Service Desk notes pattern of issues being reported that may warrant a Major Incident consideration.	**Service Desk Agent**	• Poll other SD Agents • Run ticket report • Check Change Control Calendar
2	**Notify the On-Call Technician**	**Service Desk Agent**	• Assign the ticket to the technician • Service Desk Agent and Technician Agree on a Service Desk update plan
1a	**Identify a Potential Major Incident** IT monitoring tools signal an outage that may warrant a Major Incident consideration.	**Technician**	• Engage the Incident Response Team, if necessary • Begin Investigation of potential MI • Identify the potential Incident Commander
2a	**Notify the Service Desk**	**Technician**	• Technician calls **IT Service Desk back line at 415-353-4444** and indicates incident is in under "watch". • Service Desk Agent and Technician Agree on a Service Desk update plan
3	**Notify the Service Desk Manager or designee**	**Service Desk Agent**	**After hours refer to:** http://oncall.ucsfmedicalcenter.org/ • ITSD - Manager
4	**Confirm that there is a system-wide issue**	**Technician**	• Consult with the Service Desk Manager and Agent to confirm that there is a system-wide issue • Decision: to Invoke escalation to Major Incident P2 using the following criteria: o More than a single unit or floor is affected o Received >5 more calls for the same issue within 30 minutes
4a	**Declare P2**	**Service Desk Agent**	• Received >5 more calls for the same issue within 30 minutes
5	**Invoke escalation to Major Incident (MI) (P2)**	**Service Desk Manager**	At the direction of the Service Desk Manager: • Service Desk Agent Categorizes Symptom as Major Outage (automated notification to ITS Managers and Directors)

ID	Escalation to Major Incident (P2) HIGH	Action by:	Notes
6	**Notify the Incident Commander there is a Major Incident P2**	**Technician**	AdCom On-Call Outlook Calendar • BA/Infrastructure Systems & DBA Pager Duty Calendar • Infrastructure Network Oncall
7	**Open Technical Communication Bridge,** if necessary Campus **ITS MI Technical Communication Bridge**: 353-8000, code: 602914 Med Center **MI Technical Communication Bridge**: 353-8000, PIN 650510	**Incident Commander**	• Multiple technicians involved. • Bridge facilitates faster coordination of troubleshooting**.**
8	**Incident Commander begins the Event Record and documents work plan for remediation**	**Incident Commander**	• This Record is used to note actions taken and actions planned. It is also used to debrief ITS AOC in the event that this is required • Update the incident worklog
9	**Prepare front-end ACD message** for inbound customer calls	**Service Desk Agent**	**Decision Criteria/Consideration:** • If warranted by call volume • Front end should not be used if calls are still needed for additional examples.
10	**Initiate Service Desk Communication Process:** **DECISION : Notify owners or end-users** **Email Customer-facing Notifications** and/or **Notify System Owners** and/or Application Functional Owners	**Service Desk Manager**	**Decision Criteria/Consideration:** • Specific instruction located in the KB Support Information
11	**Escalate to Priority 1** **Campus – ITS -P1** **Med Center – IT-911**	**Incident Commander**	**Evaluation Criteria/Consideration:** • Is this major incident that is affecting a large group of user or critical business processes? • Is there extreme impact to patient care and business operations? • Will the resolution of this event require additional technical resources? • Involves a Medical Center Tier 1 application? Note: Some Campus applications are considered Medical Center Tier 1 e.g . Exchange • Is greater awareness warranted? • Is ITS AOC awareness warranted?

ID	Escalation to Priority 1 (P1) CRITICAL	Action by:	Notes
12	Initiate Priority 1 Conference Bridge **Campus -** ITS -P1 353-8000, code: 271433 **Med Center –** IT-911 353-8000, PIN 911490	**Incident Commander**	
13	**Update Incident Ticket P1**	**Service Desk Manager**	At the direction of the Service Desk Manager the Service Desk Agent: • Updates the Incident to P1 Major Outage • Automated Notification to ITS Managers and Directors
14	**Notify: AOC** **Campus - ITS AOC and all relevant IT** teams/personnel as requested by the Incident Commander If this Incident involves a Medical Center Tier 1 application then the Medical Center IT AOC must be notified and the IT911 Conference Bridge activated. **Med Center – IT AOC and all relevant IT** teams/personnel as requested by the Incident Commander	**Service Desk Agent**	**Refer to:** http://oncall.ucsfmedicalcenter.org/ • Campus ITS AOC • Med Center IT AOC AdCom On-Call Outlook Calendar • BA/Infrastructure Systems & DBA Pager Duty Calendar • Infrastructure Network Oncall
15	**DECISION: Notify CIO** Briefed by phone every 30 minutes - and/or provide option of joining **ITS P1 or IT 911** conference bridge	**ITS/IT Administrator On-Call Campus (AOC)**	**Evaluation Criteria/Consideration:** • Is greater awareness to hospital operations warranted? • Would executive-level leadership benefit from greater awareness?
16	**DECISION: Cutover to Disaster Recovery Process** (if available) or **Continue with remediation efforts until Incident Commander announces that issue has been stabilized**	**Incident Commander**	**Evaluation Criteria/Consideration:** • Unresolved after 24 hours? • No recovery plan in sight?
17	**Confirm Stabilization or Resolution with affected end-users**	**Incident Commander**	
ID	**Closure/Stabilization**	**Action by:**	**Notes**
18	**Update and resolve incident ticket**	**Technician**	
19	**Remove Front-end ACD Message**	**Service Desk Agent**	
20	**Close out Service Desk Communication Process,** if necessary	**Service Desk Manager**	
21	**Complete Event Record**	**Incident Commander**	
22	**Schedule Closure Call**	**Incident Commander**	