Incident Management Process

INSIGHTSCS CORP.

JANUARY 01, 2019

Subject: **Incident Management Process**

Approved: Relly Earl Noman – CTO/CIO   Effective Date: 01 January 2019

1. INTRODUCTION

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Normal service operation is defined as service operation within service level agreement (SLA) limits.

The scope of the Incident Management process includes a standard set of processes, procedures, responsibilities and me rics that are utilized across the enterprise.

DEFINITION: An ***incident*** is any event which is not part of the standard operation of a service and which causes, or may cause an interruption to, or a reduction in the quality of that service.

The Incident Management process includes Incident Acceptance and Recording, Classification and Initial Support, Matching, Investigation and Diagnosis, Resolution and Recovery, Closure, and Progress Monitoring and Reporting

2. ROLES AND RESPONSIBILITIES

2.1. CUSTOMER

- Identifies incident
- Confirms incident has been resolved

2.2. SERVICE DESK – 1ST LEVEL SUPPORT

- First point of contact for customers reporting service disruption of service. For InsightSCS these would be members of the Support Desk and/or the Implementation Team.
- Responsible for recording and classifying incidents and undertaking an immediate effort in order to restore a failed IT service as quickly as possible
- Transfer incidents to expert technical support when no ad-hoc solution can be achieved
- Provide customer updates as required
- the Service Desk can be accessed online here: https://insightsupplychain.atlassian.net/servicedesk/customer/portals

2.3. 2ND LEVEL SUPPORT

- Takes over incident which cannot be solved immediately by Level 1 Support
- Responsible for incident investigation, diagnosis and recovery within defined priorities
- Request external support if necessary
- Aim to restore an IT service as quickly as possible
- Transfer incidents to Level 3 support when no solution can be found
- Provide customer updates as required

2.4. 3RD LEVEL SUPPORT

- Typically located at hardware or software manufacturers.
- Serv ces are requested by 2nd Level Support if required for solving anIncident.Responsible for incident investigation, diagnosis and recovery within defined priorities
- Aim to restore an IT service as quickly as possible
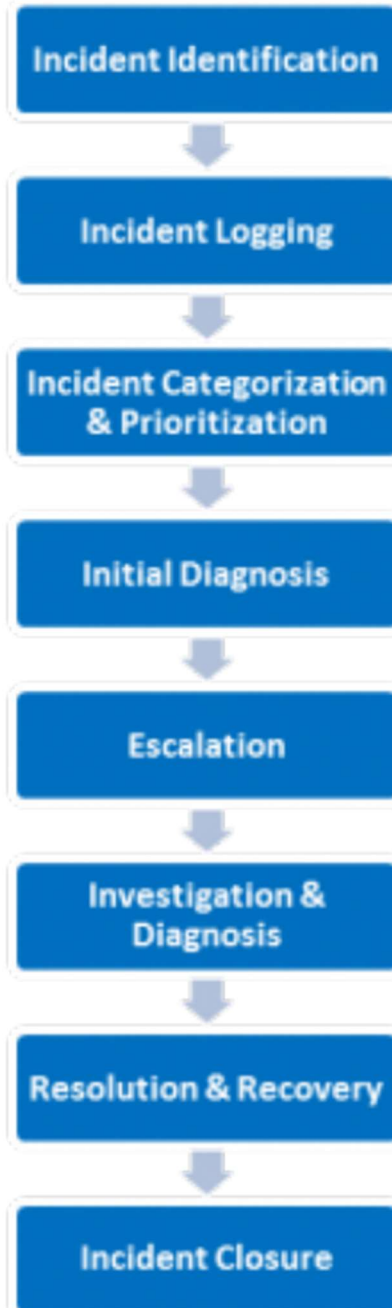
2.5. MAJOR INCIDENT TEAM

- A dynamically established team formulated to concentrate on the resolution of a major incident
- Initiates the Event Communication Process
- Initiates the Problem Management Process
- Conducts SWAT session after event

2.6. INCIDENT MANAGER – PROCESS OWNER

- Manages the effective implementation of the Incident Management Process
- Makes recommendations for process improvement
- Generates Incident Management performance reports
- Represents the first stage of escalation for incidents which are not resolved within the agreed Service Levels

3. PROCESS DEFINITION

3.1. Enterprise Incident Management High Level Process Map

4. ENTRY CRITERIA

- Incident report

5. PROCEDURE

ID	Step	Responsibility
	Incident Logging and Categorization Sub-Process	
ID	Step	Responsibility
1	**Detect Incident** Identify a disruption of service.	▪ Customer
2	**Contact Service Desk or Implementation Team Lead/Contact Person** Customer contacts the Service Desk to report a disruption in service or request service.	▪ Customer
3	**Type?** Incident – go to step 4 / Service Request – Hand off to Service Request Process	▪ Service Desk
4	**Open Incident Ticket (classified at User Service Request)** Upon receiving a call (or request) from a Customer, the Service Desk Analyst enters the Customer and incident information into the ticket.	▪ Service Desk
	Hand-off to Service Request Process	
	Monitor and Track Incidents The Incident Manager is responsible for monitoring and tracking incident throughout the process.	▪ Incident Manager
5	**Assign: Impact, Urgency, Priority** Using the impact, urgency, priority matrix, determine and set the priority for the incident. Setting the priority begins the "clock" for the Service Level Agreement (SLA) associated with that priority. At this point, Service Desk Analyst becomes the Ticket Owner.	▪ Service Desk
	Immediate Incident Resolution by Level 1 Sub-Process	
6	**Check Support Matrix, Documentation, Solutions Database and Configuration items** Review all available information for known errors and solutions to similar incidents.	▪ Service Desk
7	**Document Steps Taken** Update the worklog in the Incident Ticket with all of the troubleshooting steps taken to resolve the incident so far.	▪ Service Desk
8	**Resolve?** Yes – go to step9 / No – go to step 11	▪ Service Desk
9	**Notify Customer**	▪ Service Desk
10	**Valid?** Yes – go to step 24 / No – go to step 8	▪ Customer
11	**Triage** The Service Desk Analyst assigns the Incident ticket to Level 2 Support. At this stage the responsibility for resolving the incident and communicating with the Customer passes to the assigned Support Analyst however, the responsibility for final customer contact and closure of the incident remains with the Service Desk Analyst.	▪ Service Desk
12	**System Event?** Yes – go to step Initiate Major Incident Management Procedures / No – go to step 13	▪ Service Desk

	Initiate Major Incident Management Sub-Process		
	Monitor and Track Event The Event Manger is responsible for initiating the Communication Management Process and the Problem Management process as need. They are also responsible for tracking the event to resolution.		▪ Incident Manager

Immediate Resolution by Level 2 Sub-Process

ID	Step	Responsibility
13	**Review Incident Ticket** Review the incident in order to understand the issue. Consult the Problem Management Database for known errors. If necessary, contact the Customer, IT Support Unit or the Service Desk to gain further clarity of the incident. Begin diagnosis of the incident.	▪ Level 2 Support
14	**Resolve?** Yes – go to step 15/ No – go to step 18 Determine if the incident can be resolved without making any system update and inform the customer of the solution. When the Level 2 Support Analysis is unable to resolve the incident it is escalated to Level 3 Support.	▪ Level 2 Support
15	**Implement Solution and Resolve Incident** Resolve the incident by implementing the necessary solution.	▪ Level 2 Support
16	**Update Incident Ticket and Notify Customer** Document the resolution in the Incident Ticket and enter the closure code. Contact the Customer with the solution to the incident	▪ Level 2 Support
17	**Valid?** Yes – go to step 24 / No - go to step 14	▪ Customer ▪ IT Support Group
18	**Update Incident Ticket and Triage to Level 3** Document the steps taken to diagnose/resolve the incident in the worklog of the Incident Ticket. When the Level 2 Support Analyst is unable to resolve the incident it is triaged to Level 3 Support. At this stage the responsibility for resolving the incident and communicating with the Customer passes to the assigned Support Analyst.	▪ Level 2 Support
19	**Review Incident Ticket** Review the incident in order to understand the issue. Consult the Problem Management Database for known errors. If necessary, contact the Customer, IT Support Unit or the Service Desk to gain further clarity of the incident. Begin diagnosis of the incident.	▪ Level 3 Support
20	**Resolve?** Yes – go to step 32 / No – hand-off to Escalation Process and/or Change Management Process and/or Problem Management The Level 3 Support Analyst determines if the incident can be resolved without making any system updates and informs the customer of the solution. If system updates are required the Level 3 Support Analyst will initiate the Change Management process	▪ Level 3 Support
	Initiate Monitoring and Escalation Sub-Process	
	Initiate Change Management Process	
	Initiate Problem Management Process	
21	**Implement Solution and Resolve Incident** The Level 3 Support Analyst resolves the incident by implementing the necessary solution.	▪ Level 3 Support

22	**Update Incident Ticket and Notify Customer** Document the resolution in the Incident Ticket and enter the closure code. Contact the Customer with the solution to the incident.	▪ Level 3 Support
23	**Valid?** Yes – go to step 24 / No go to step 20	▪ Customer ▪ IT Support Group

Incident Closure & Evaluation Sub-Process		
ID	**Step**	**Responsibility**
24	**Close Incident Ticket** The Ticket Assignee is responsible for closure of the Incident Ticket.	▪ Service Desk ▪ Level 2 Support ▪ Level 3 Support
25	**Generate Incident Report, including Performance Metrics**	▪ Incident Manager
26	**Evaluate Performance Metrics Against SLA**	▪ Incident Manager
27	**Conduct Performance Review**	▪ Incident Manager

6. EXIT CRITERIA

- Incident has been resolved to customer's satisfaction or has been handed off to another process.

7. INCIDENT LOGGIN AND CATEGORIZATION SUB-PROCESS

7.1. Sub-Process Objective

Incident Logging and Categorization is a sub-process of the Incident Management Process. Its objective is to record and prioritize the Incident with ap**p**ropriate diligence, in order to facilitate a swift and effective resolution.

7.2. Logging Incidents

Incident Logging and Categorization is a sub-process of the Incident Management Process. Its objective is to record and prioritize the Incident with ap**p**ropriate diligence, in order to facilitate a swift and effective resolution.

An Incident Record m st contain the following information:

1. Unique ID of the Incident (usually allocated automatically by the system)

2. Date and time of recording

3. Service Desk agent responsible for the registration

4. Caller / user data

5. Description of symptom

7.3.   Prioritization Of Incidents

Three metrics are used for determining the order in which incidents are processed. Incident priority is assigned when the Ticket is opened and is determined primarily on the basis of urgency and impact.

- Impact - The effect or scope that an incident has.

- Urgency - The speed at which the incident should be resolved.

- Priority – The combined value of the Impact and Urgency.

IMPACT TABLE

RANK	DESCRIPTION
1. Extensive/ Widespread:	Clinical Definition: Multiple Patients Non-Clinical Definition: Entire department, floor, branch, line of business, external customer
2. Significant/ Large:	Clinical Definition: One Patient Non-Clinical Definition: Greater than 5 business people
3. Moderate/ Limited:	Clinical Definition: No Patient Impact Non-Clinical Definition: Less than 5 business people affected.
4. Minor/ Localized:	Clinical Definition: No Patient Impact Non-Clinical Definition: 1 business person affected.

URGENCY TABLE

RANK	DESCRIPTION
1. High:	Process stopped; customer cannot work. System and/or service is unavailable. Generally customers are unable to work and no workaround is available
2. Medium:	Process affected; certain functions are unavailable to customers. System and/or service are degraded. May or may not have workaround available.
3. Low:	Process affected; certain functions are unavailable to customers. The work can be scheduled. System and/or service. Inconvenienced but still available (Work, Excel, etc). Workaround available.

8. INCIDENT MONITORING AND ESCALATION SUB-PROCESS

8.1. Sub-Process Objective

Incident Monitoring and Escalation is a sub-process of the Incident Management Process. The objective of this process is the continuous monitoring of outstanding incidents so that countermeasures may be introduced as soon as possible if service levels are likely to be breached.

8.2. Incident Management Service Levels

Priority	Description	Response Time	Target Resolution Time
1. System Down	The system is inoperable due to system failure.	1 hours	Within 2 hours - we will initiate a live call with the technical groups until the issue is resolved.
2. Critical	A major function is affected by a software failure, or administrative/trainin g issue diminishing productivity.	2 hours	Within 4 hours - we will assign as many support specialists as needed along with the best workaround available.
3. High	A minor program function is affected by a software error, resulting in reducing productivity, or a problem occurs infrequently.	4-6 hours	if a workaround can be provided, the correction will be scheduled for the next regular upgrade, if not, a correction will be typically provided within 5-7 days.
4. Medium	A desired new functionality is not working as expected, or a problem occurs that is not readily reproducible.	12 hours	if a workaround can be provided, the correction will be scheduled for the next regular upgrade, if not, a correction will be typically provided within 2 weeks.
5. Low	An issue with negligible impact.	24 hours	if a workaround can be provided, the correction will be made based on agreed upon relevance.

8.3. Escalation

Escalation of an incident can take place at any time and at any support level in the resolution process, as defined in the Service Level Agreement.

- Functional escalation – involving personnel with more specialist skills, time or access privileges to solve the incident.

- Hierarchical escalation – involving a higher level of organization authority, when it appears that the current level of authority is insufficient to ensure that the incident will be resolved in time and/or satisfactorily.

8.4.   Service Desk Response Times

The following Priority Chart shows response time after initial Assessment/Assignment and creation of a ticket by the Service Desk (10 to 30 minutes.) Times are measured in clock hours and/or minutes unless otherwise specified. If a ticket is initiated by a telephone call, it will be created within 10 minutes; if initiated by eMail, the ticket will be created within 48 hours.

- The **Target Incident Response Acknowledgement Time** is the time the Service Desk has to respond to the customer to acknowledge receipt of the ticket and that it is being actively worked.
- The **Target Status Update Time** is the time interval the assigned group/individual has to update the Service Desk on ticket status.
- The **Customer Status Update Time** is the interval that the Service Desk has to update the customer on ticket status.
- The **Target Resolution Time** is the total time from ticket creation to resolve the incident and restore service to the user.
- The **Target Percentage of Calls Resolved on Time** is the percentage of calls that meet the priority time frame criteria.

Incident Priority Chart

Priority	Target Incident Response Acknowledgement Time (*to customer from the Service Desk*)	Target Status Update Time (*to Service Desk from assigned group/person*)	Customer Status Update Time Goal	Target Resolution Time	Target % of Call Resolved on Time
Critical	15 minutes	Within 15 minutes, then every hour by the assigned working team until resolution has been achieved or identified	Service Desk will: • Provide initial communication within 60 min • Update Service Alert Page every 60 min • Send resolution notice	1 hour	90%
High	1 hour	Within 1 hour, then every 2 hours thereafter by the assigned working team until resolution has been achieved or identified	Service Desk will: • Provide initial communication within 60 min • Update Service Alert Page every 60 min • Send resolution notice	2 hours	90%
Medium	24 hours	Within 3 hours	Service Desk will provide status upon request	3 business days	80%
Low	24 hours	Within 1 business day	Service Desk will provide status upon request	5 business days	80%