



Process Document

Incident Management Process

Document Owner	Information Technology
Approving Manager	[Redacted]
Approved Date	6/6/2023
Revision Date	N/A
Content Review Cycle	6/6/2025
SharePoint Location	[Redacted] Knowledge Hub / Processes / Incident Management Process



Table of Contents

Table of Contents 2

Introduction 3

Purpose 3

Process Summary 3

Roles and Responsibilities..... 4

 RACI Chart 5

Incident Support Guidelines 6

 Incident Breakdown and SLA Chart 6

 Support Hours 7

 [Redacted] Tier 1 Support..... 7

 Tier 2 and Tier 3 Support 7

 Escalations..... 7

Process Flowchart 8

Process Description..... 9

 Incident Raising & Documentation 9

 Triage 10

 Troubleshooting..... 12

 Resolution 14

Associated Documents..... 15

Definitions 15

Contributors to This Document 16

Revision History 17

Record of Approvals..... 17



Introduction

The **Incident Management Process** applies to all [Incidents](#) (unplanned interruptions to or reductions in the quality of an IT Service or failures of [Configuration Items \[CIs\]](#) that have not yet affected a service).

[Redacted] (aka the Tier 1 Service Desk) is the initial line of support for all IT Incidents. Incidents may be reported to [Redacted] through the online [\[Redacted\] Portal](#) (preferred), by phone, or by email. Although the other methods are preferable, Incidents may also be reported via Microsoft Teams chat. Incidents raised through these or any other means must be entered by **[Redacted] (Tier 1)** as a new Incident ticket in [Redacted], the system of record.

- **Tier 1 (Redacted)** collects details, determines the Incident's priority, and troubleshoots the issue
- **Tier 2 (End User Support [EUS] and Unified Communications and Collaboration [UCC])** troubleshoots Incidents beyond Tier 1 expertise
- **Tier 3 (Administrators/Developers/Subject Matter Experts [SMEs])** troubleshoots Incidents beyond Tier 1 and 2 expertise and/or access

Notes:

- The [Change Request \(CHG\)](#) process should be followed where applicable.
- **[Redacted]** is responsible for troubleshooting application-related incidents; can be Tier 2 or 3

Purpose

The purpose of this process is to ensure that multiple [Redacted] teams work together effectively to troubleshoot and resolve Incidents to restore normal operation to affected services ([Service Restoration](#)) as soon as possible within the specified [Service Level Agreements \(SLAs\)](#).

Process Summary

When an Incident occurs, a **Requestor** contacts **[Redacted] (Tier 1)**, who documents the Incident in a *[Redacted]* Incident Ticket. Depending on the [Incident Category](#), Tier 1 either restores service or escalates the ticket to **Tier 2** (for a complex Incident impacting end-users) or **Tier 3** (for a system, infrastructure, or Enterprise Service Incident) for troubleshooting and service restoration (Tier 2 may also escalate an Incident to Tier 3 for assistance if unable to resolve). Once service is restored, the Incident Ticket is documented with the resolution and closed.



Roles and Responsibilities

Role	Responsibilities
Communications	<ul style="list-style-type: none">Send [Redacted] Alert emails and/or EverBridge text messagesCreates a [Redacted] site banner alert for incidents
External Vendors	<ul style="list-style-type: none">Works with Tier 3 to resolve Incidents when necessary
Incident Owner	<ul style="list-style-type: none">Designated Tier 1/Tier 2/Tier 3 team member or Watch Officer (or Incidents that occur outside of business hours) or who owns the Incident and leads its resolutionCapture information pertaining to the Incident, e.g., stakeholders engaged and action needed for recoveryTriage/coordinate & lead resolution effortsMaintain a general overview of the IncidentAct as generalist who understands multiple affected areas
[Redacted] Watch Officer	<ul style="list-style-type: none">Monitor and respond to Incidents that occur outside of business hours during their scheduled week of service
Process Owner	<ul style="list-style-type: none">Primary person who owns the Incident process and approves any changes to the process
Requestor	<ul style="list-style-type: none">Report Incident and details to the Service DeskAvailable for further info or validation of restored service
Tier 1 - [Redacted]	<ul style="list-style-type: none">Collect Incident details from the customer/requestor & capture specific info based on the ticketDetermine Incident priority (major or minor) and troubleshootEscalate Incident to Tiers 2 (for complex issues) or 3 (usually for systems issues) when the Incident is beyond Tier 1 expertise and/or access
[Redacted]	<ul style="list-style-type: none">Troubleshoot application-related incidents
Tier 2 - End User Support (EUS) and Unified Communications and Collaboration (UCC)	<ul style="list-style-type: none">Troubleshoot Incidents escalated from Tier 1Explain Incident resolution via Knowledge Article, triage with Tier 1Escalate Incident to Tier 3 when the Incident is beyond Tier 2 expertise and/or access (usually for systems issues)
Tier 3 – Administrators / Developers / Subject Matter Experts (SMEs)	<ul style="list-style-type: none">Troubleshoot Incidents escalated from Tiers 1 or 2Help identify, contact, and work with alternate resource(s) if unable to resolve, e.g., they will open up tickets with external vendors for professional support if unable to resolveCommunicate technical findings as neededRemain engaged until resolution or until other technical resources can take over dutiesComplete Change Request (CHG) documentation



RACI Chart

Tasks	Roles									
R = Responsible A = Accountable C = Consulted I = Informed	Communications	Requestor	[REDACTED] Watch Officer	Tier 1 (Redacted) Leadership	Tier 1 (Redacted)	Tier 2 (EUS, UCC, [Redacted])	Tier 3 & [Redacted] SMEs	External Vendors	Incident Owner	Process Owner
Report Incidents		A/R	I	I	I					
Respond to Major Incidents During Non-Business Hours	I		R				C		A	
Respond to Non-Business Hours VIP/UCC Support Incidents During Non-Business Hours			R			C			A	
Collect Incident Details/Create Ticket		C	I	I	I				A/R	
Create Problem Tickets	I	I	I	A/R	I	I	I		I	
Escalate Complex End User Incidents to Tier 2 or [Redacted]		I		I	R	I			A	
Escalate System, Infrastructure, or Enterprise Service Incidents to Tier 3	I	I	I	I	I	R			A	
Escalate Complex System, Infrastructure, or Enterprise Service Incident to external vendor	I	I	I	I	I	I	R		A	
Send Alerts for Major Incidents	A/R		I	I	I	I	C		I	
Create a [Redacted] site banner alert for incidents	A/R	I	I	I	I	I	I		I	I
Resolve/Document Minor End User Incidents		I		I	R				A	
Resolve/Document Complex End User Incidents	I	I	I	I	I	R			A	
Resolve/Document System, Infrastructure, or Enterprise Service Incidents	I	I	I	I	I	I	R		A	
Resolve Complex System, Infrastructure, or Enterprise Service Incidents	I	I	I	I	I	I	I	R	A	
Confirm Resolution/Service Restoration	I	C/R	I	I	I	I	I		A	I
Approve Process Changes	I			I	I	I	I		I	A/R
Create, Modify, and Ensure Process Compliance	I			I	I	I	I		I	A/R



Redacted

6/6/2023

Incident Support Guidelines

Incident Breakdown and SLA Chart

The below chart defines Incidents and the corresponding SLAs by **Priority Level** (from P1 [highest] to P5 [lowest]), **Category** ([Major](#) vs [Minor](#)), **Priority / Impact and Description**, **Target Response Time**, **Target Resolution Time**, and **Service Target %** (the target percentage of Incident responses and/or resolutions that will meet the defined goal).

Notes:

- The *[Redacted]* Tier 1 and Tier 2/Tier 3 [OLAs \(Operational Level Agreements\)](#) have been combined to create the total SLAs
- The *[Redacted]* Tier 1 **Target Resolution Times** below are estimates only and are not indicative of their contract
- The below chart may differ from the after-hours SLAs as defined in the [Watch Officer Triage Procedure](#)

Category /Priority #		Priority / Impact & Description	Target Response Time		Target Resolution Time	Service Target %
Major Incidents	P1	Critical Priority/High Impact: Major production or critical system outage. Applies to site / multi-site / region / company-wide incidents.	[Redacted] T1 - Phone	30 Secs	12 Hours	95%
			[Redacted] T1 - Email or Portal	2 Hours	12 Hours	90%
			Tier 2 / Tier 3 - Escalation	30 Mins	12 Hours	95%
			Total	2.5 Hours	24 Hours	95%
	P2	High Priority/Limited Impact: Partial outage or degradation of services. Applies to team / group / department-wide incidents.	[Redacted] T1 - Phone	30 Secs	1 Day	95%
			[Redacted] T1 - Email or Portal	2 Hours	1 Day	90%
			Tier 2 / Tier 3 - Escalation	2 Hours	1 Day	95%
			Total	4 Hours	2 Days	95%
Minor Incidents	P3	Medium Priority/High-Low Impact: Issue with production environment preventing a limited number of staff from completing work. Should be working and the urgency is a medium level.	[Redacted] T1 - Phone	30 Secs	2 Days	95%
			[Redacted] T1 - Email or Portal	2 Hours	2 Days	90%
			Tier 2 / Tier 3 - Escalation	1 Day	2 Days	95%
			Total	1 Day	4 Days	95%
	P4	Low Priority/High Impact: Minimal users are experiencing a minor issue; however, ability to perform daily work is not impacted.	[Redacted] T1 - Phone	30 Secs	5 Days	95%
			[Redacted] T1 - Email or Portal	2 Hours	5 Days	90%
			Tier 2 / Tier 3 - Escalation	3 Days	5 Days	95%
			Total	3 Days	10 Days	95%
	P5	Low Priority/Low Impact: One user is experiencing an issue. Does not impact 100% of job function.	[Redacted] T1 - Phone	30 Secs	10 Days	95%
			[Redacted] T1 - Email or Portal	2 Hours	10 Days	90%
			Tier 2 / Tier 3 - Escalation	5 Days	10 Days	95%
			Total	5 Days	20 Days	95%



Redacted

6/6/2023

Incident Support Guidelines, continued

Support Hours

[Redacted] Tier 1 Support

- [Redacted] (Tier 1) Help Desk support hours are from Monday to Thursday from 7:00 AM – 8:00 PM EST and on Friday from 7:00 AM – 6:00 PM EST

Tier 2 and Tier 3 Support

- **Minor incidents (P3, P4, and P5):** Core business hours: Monday to Friday 8:00 AM – 5:00 PM EST
- **Major incidents (P1 and P2):** 24 hours a day, 7 days a week, including during [REDACTED] holidays
 - **Important:** The on-duty [Redacted] [Watch Officer](#) handles response coordination for Major or VIP End-User/UCC Support Incidents that occur outside of core business hours until they are resolved or handed off to the appropriate team at the beginning of the following business day. See the [Watch Officer Triage Procedure](#) for additional information.

Escalations

- Ticket escalation paths and resolution times are contingent on the incident priority level as noted in the [Incident Breakdown and SLA Chart](#). The below should be used as a guide:
 - If an Incident requires escalation beyond [Redacted] (Tier 1):
 - **Tier 2 End User Support (EUS)** is the POC for laptop, laptop accessory, or software-related escalations
 - **Unified Communications and Collaboration (UCC)** is the POC for telecommunications or desktop peripheral-related escalations
 - **Infrastructure (Servers)** is the POC for Infrastructure Server-related escalations
 - **Infrastructure (Network)** is the POC for network-related escalations
 - **M365 & Cloud App Services** is the POC for M365 Cloud Apps related escalations
 - **Endpoint Services** is the POC for Endpoint Services-related escalations
 - **Cloud Services** is the POC for cloud-related escalations
 - **[Redacted]** is the POC for application-related escalations
 - Incidents beyond the scope of the above leads are to be escalated to the [REDACTED] Supervisor

Important: The on-duty [Redacted] Watch Officer is responsible for coordinating the escalation for Major or VIP End-User/UCC Support Incidents that occur outside of core business hours. See the [Watch Officer Triage Procedure](#) for additional information.



Redacted

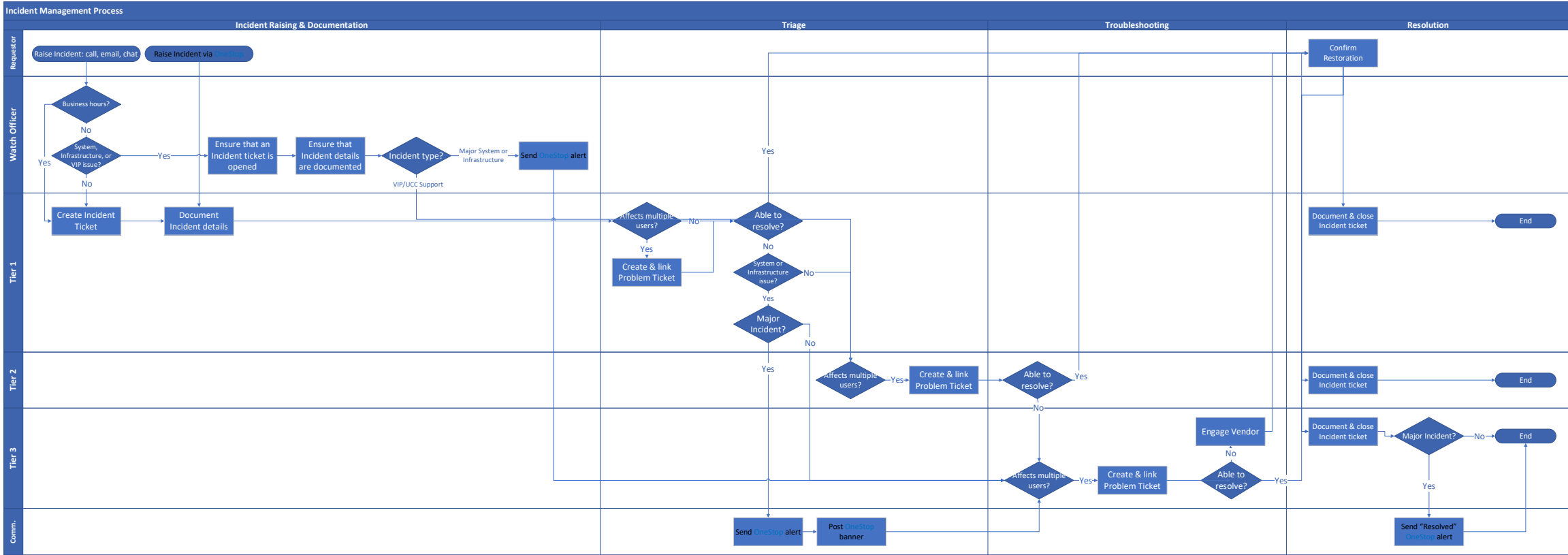
Incident Management Process

Process Document

6/6/2023

Process Flowchart

The below flowchart summarizes the Incident Management Process. The [Process Description](#) section contains more detailed information about the steps taken by each team during the process.





Redacted

6/6/2023

Process Description

Incident Raising & Documentation

Step	Action								
1.	<p>Proceed based on the nature and timing of the Incident:</p> <table> <tr> <th>If...</th><th>Then...</th></tr> <tr> <td>A Requestor reports an IT Incident via the [Redacted] Portal (preferred method, as this automatically creates a [Redacted] ticket), call, or email <u>during normal business hours</u>.</td><td>The assigned Tier 1 Analyst becomes the Incident Owner. Continue to Step 2. Note: Requestors occasionally reach out to [Redacted] (Tier 1) via <i>Microsoft Teams</i> chat in lieu of the above methods.</td></tr> <tr> <td>A VIP End-User/UCC Support or a <u>system, infrastructure, or Enterprise Service</u> Incident occurs <u>outside of normal business hours</u></td><td>The [Redacted] Watch Officer becomes the Incident Owner. Continue to Step 2. Note: See the <u>Watch Officer Triage Procedure</u> for additional after-hours Incident information.</td></tr> </table>	If...	Then...	A Requestor reports an IT Incident via the [Redacted] Portal (preferred method, as this automatically creates a [Redacted] ticket), call, or email <u>during normal business hours</u> .	The assigned Tier 1 Analyst becomes the Incident Owner. Continue to Step 2. Note: Requestors occasionally reach out to [Redacted] (Tier 1) via <i>Microsoft Teams</i> chat in lieu of the above methods.	A VIP End-User/UCC Support or a <u>system, infrastructure, or Enterprise Service</u> Incident occurs <u>outside of normal business hours</u>	The [Redacted] Watch Officer becomes the Incident Owner. Continue to Step 2. Note: See the <u>Watch Officer Triage Procedure</u> for additional after-hours Incident information.		
If...	Then...								
A Requestor reports an IT Incident via the [Redacted] Portal (preferred method, as this automatically creates a [Redacted] ticket), call, or email <u>during normal business hours</u> .	The assigned Tier 1 Analyst becomes the Incident Owner. Continue to Step 2. Note: Requestors occasionally reach out to [Redacted] (Tier 1) via <i>Microsoft Teams</i> chat in lieu of the above methods.								
A VIP End-User/UCC Support or a <u>system, infrastructure, or Enterprise Service</u> Incident occurs <u>outside of normal business hours</u>	The [Redacted] Watch Officer becomes the Incident Owner. Continue to Step 2. Note: See the <u>Watch Officer Triage Procedure</u> for additional after-hours Incident information.								
2.	<p>The Incident Owner creates a [Redacted] ticket for the Incident if one has not been created by the Requestor via the [Redacted] portal.</p> <p>Note: The [Redacted] Watch Officer is responsible for reaching out to the appropriate team to help create and document after-hours Incident tickets.</p>								
3.	The Incident Owner collects specific Incident details and captures them within the ticket.								
4.	<p>Proceed based on the nature and timing of the Incident:</p> <table> <tr> <th>If the Incident Occurred...</th><th>Then...</th></tr> <tr> <td><u>During</u> normal business hours</td><td>The Incident Owner (in this case, the assigned Tier 1 Analyst) continues to Step 5 (Triage).</td></tr> <tr> <td><u>Outside of</u> normal business hours and is a VIP End-User/UCC Support issue</td><td>The Incident Owner (in this case, the [Redacted] Watch Officer) reaches out to Tier 2 for assistance. Continue to Step 9 (Troubleshooting).</td></tr> <tr> <td><u>Outside of</u> normal business hours and is a <u>major system, infrastructure, or Enterprise Service</u> issue</td><td>The Incident Owner (in this case, the [Redacted] Watch Officer) sends a [Redacted] Alert email and/or EverBridge text explaining the service disruption to the affected parties and reaches out to Tier 3 for assistance. Continue to Step 11 (Troubleshooting).</td></tr> </table>	If the Incident Occurred...	Then...	<u>During</u> normal business hours	The Incident Owner (in this case, the assigned Tier 1 Analyst) continues to Step 5 (Triage) .	<u>Outside of</u> normal business hours and is a VIP End-User/UCC Support issue	The Incident Owner (in this case, the [Redacted] Watch Officer) reaches out to Tier 2 for assistance. Continue to Step 9 (Troubleshooting) .	<u>Outside of</u> normal business hours and is a <u>major system, infrastructure, or Enterprise Service</u> issue	The Incident Owner (in this case, the [Redacted] Watch Officer) sends a [Redacted] Alert email and/or EverBridge text explaining the service disruption to the affected parties and reaches out to Tier 3 for assistance. Continue to Step 11 (Troubleshooting) .
If the Incident Occurred...	Then...								
<u>During</u> normal business hours	The Incident Owner (in this case, the assigned Tier 1 Analyst) continues to Step 5 (Triage) .								
<u>Outside of</u> normal business hours and is a VIP End-User/UCC Support issue	The Incident Owner (in this case, the [Redacted] Watch Officer) reaches out to Tier 2 for assistance. Continue to Step 9 (Troubleshooting) .								
<u>Outside of</u> normal business hours and is a <u>major system, infrastructure, or Enterprise Service</u> issue	The Incident Owner (in this case, the [Redacted] Watch Officer) sends a [Redacted] Alert email and/or EverBridge text explaining the service disruption to the affected parties and reaches out to Tier 3 for assistance. Continue to Step 11 (Troubleshooting) .								

Continued on next page



Redacted

6/6/2023

Process Description, continued

Triage

Step	Action	
5.	The Tier 1 Analyst assesses, troubleshoots, and attempts to resolve the Incident.	
	Note: They will research related Knowledge Articles (KAs) for additional information as necessary.	
	If the Tier 1 Analyst...	Then they...
	Is <u>able</u> to resolve the Incident	Resolve the incident. Continue to Step 17.
	Is <u>unable</u> to resolve the Incident	Reach out for assistance via the <i>[Redacted] Tier 1 Microsoft Teams Channel</i> or the <i>Federal Leadership Channel</i> . Continue to Step 6.
6.	Tier 1 Leadership proceeds based on the below chart:	
	If...	Then...
	Three or more Incident tickets are <u>created</u> due to end users/customers encountering the same issue or if the incident has the <u>potential to affect multiple users</u>	Tier 1 Leadership creates a Problem Ticket in [Redacted] to capture the increase of tickets / trend analysis and links all pertinent incidents to it. Continue to Step 7. Note: One parent Problem Ticket can respond to and resolve all linked child Incidents.
	The issue will only affect one or a few users	Continue to Step 7.
7.	Tier 1 Leadership assesses the Incident’s severity and proceeds based on the chart below:	
	If the Incident...	Then...
	<u>Does not require</u> additional expertise	Tier 1 Leadership assists the Tier 1 Analyst to resolve the Incident. Continue to Step 17.
	<u>Requires</u> additional expertise	Continue to Step 8.

Continued on next page



Redacted

6/6/2023

Process Description, continued

Step	Action								
8.	The Tier 1 Analyst proceeds based on the chart below:								
	<table><tr><th>If the Incident...</th><th>Then...</th></tr><tr><td>Requires additional expertise due to a complex <u>end-user issue</u></td><td>The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 2 department (e.g., End User Support) that can help resolve the issue. Continue to Step 11.</td></tr><tr><td>Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u> involving a <u>site, multi-site, region, or company-wide major production or critical system outage OR a team, group, or department-wide partial outage or degradation of services</u></td><td><i>The Incident is designated as Major.</i> The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 9.</td></tr><tr><td>Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u> that may or may not prevent a small number of staff from completing work.</td><td><i>The Incident is designated as Minor.</i> The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 14.</td></tr></table>	If the Incident...	Then...	Requires additional expertise due to a complex <u>end-user issue</u>	The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 2 department (e.g., End User Support) that can help resolve the issue. Continue to Step 11.	Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u> involving a <u>site, multi-site, region, or company-wide major production or critical system outage OR a team, group, or department-wide partial outage or degradation of services</u>	<i>The Incident is designated as Major.</i> The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 9.	Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u> that may or may not prevent a small number of staff from completing work.	<i>The Incident is designated as Minor.</i> The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 14.
	If the Incident...	Then...							
	Requires additional expertise due to a complex <u>end-user issue</u>	The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 2 department (e.g., End User Support) that can help resolve the issue. Continue to Step 11.							
	Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u> involving a <u>site, multi-site, region, or company-wide major production or critical system outage OR a team, group, or department-wide partial outage or degradation of services</u>	<i>The Incident is designated as Major.</i> The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 9.							
Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u> that may or may not prevent a small number of staff from completing work.	<i>The Incident is designated as Minor.</i> The Tier 1 Analyst performs a warm handoff (by escalating the incident to the relevant group's distribution list via Teams chat and reassigning the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 14.								
	Note: The assigned Tier 2 or 3 member now assumes the Incident Owner role.								
9.	The Incident Owner engages Communications to send a [Redacted] Alert email and/or EverBridge text explaining the service disruption to the affected parties. Note: The Technical Writer is Bcc'd on the email as a part of [Redacted].								
10.	Communications (the Technical Writer) creates a [Redacted] banner alert informing visitors to the site about the incident. Continue to Step 14.								

Continued on next page



Redacted

6/6/2023

Process Description, continued

Troubleshooting

Step	Action								
11.	The Tier 2 Team Member reviews the Incident notes in [Redacted] to familiarize themselves with the Incident.								
12.	<table><tr><td colspan="2">The Tier 2 Team Member proceeds based on the below chart:</td></tr><tr><th>If...</th><th>Then...</th></tr><tr><td>Three or more Incident tickets are created due to end users/customers encountering the same issue or if the incident has the potential to affect multiple users</td><td>The Tier 2 Team Member creates a Problem Ticket in [Redacted] to capture the increase of tickets / trend analysis, links all pertinent incidents to it, and informs Tier 1 Leadership of the Problem Ticket. Continue to Step 13.</td></tr><tr><td>The issue will only affect one or a few users</td><td>Continue to Step 13.</td></tr></table>	The Tier 2 Team Member proceeds based on the below chart:		If...	Then...	Three or more Incident tickets are created due to end users/customers encountering the same issue or if the incident has the potential to affect multiple users	The Tier 2 Team Member creates a Problem Ticket in [Redacted] to capture the increase of tickets / trend analysis, links all pertinent incidents to it, and informs Tier 1 Leadership of the Problem Ticket. Continue to Step 13.	The issue will only affect one or a few users	Continue to Step 13.
The Tier 2 Team Member proceeds based on the below chart:									
If...	Then...								
Three or more Incident tickets are created due to end users/customers encountering the same issue or if the incident has the potential to affect multiple users	The Tier 2 Team Member creates a Problem Ticket in [Redacted] to capture the increase of tickets / trend analysis, links all pertinent incidents to it, and informs Tier 1 Leadership of the Problem Ticket. Continue to Step 13.								
The issue will only affect one or a few users	Continue to Step 13.								
13.	<table><tr><td colspan="2">The Tier 2 Team Member assesses, troubleshoots, and attempts to resolve the Incident.</td></tr><tr><th>If the Incident...</th><th>Then...</th></tr><tr><td><u>Does not require</u> additional expertise</td><td>They resolve the Incident and triage with Tier 1 to explain the resolution (possibly including Knowledge Article creation for future Incident resolution). Continue to Step 17.</td></tr><tr><td>Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u></td><td>They perform a warm handoff (via Teams chat and reassignment of the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 14.</td></tr></table>	The Tier 2 Team Member assesses, troubleshoots, and attempts to resolve the Incident.		If the Incident...	Then...	<u>Does not require</u> additional expertise	They resolve the Incident and triage with Tier 1 to explain the resolution (possibly including Knowledge Article creation for future Incident resolution). Continue to Step 17.	Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u>	They perform a warm handoff (via Teams chat and reassignment of the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 14.
The Tier 2 Team Member assesses, troubleshoots, and attempts to resolve the Incident.									
If the Incident...	Then...								
<u>Does not require</u> additional expertise	They resolve the Incident and triage with Tier 1 to explain the resolution (possibly including Knowledge Article creation for future Incident resolution). Continue to Step 17.								
Requires additional expertise or access due to a <u>system, infrastructure, or Enterprise Service issue</u>	They perform a warm handoff (via Teams chat and reassignment of the [Redacted] ticket) to the specific Tier 3 department (e.g., Platforms/Infrastructure, [Redacted]) that can help resolve the issue. Continue to Step 14.								
14.	The assigned Tier 3 Subject Matter Expert (SME) reviews the Incident notes in [Redacted] to familiarize themselves with the Incident.								



Redacted

6/6/2023

Process Description, continued

Step	Action						
15.	The Tier 3 SME proceeds based on the below chart:						
	<table><tr><th>If...</th><th>Then...</th></tr><tr><td><u>Three or more Incident tickets are created</u> due to end users/customers encountering the same issue or if the incident has the <u>potential to affect multiple users</u></td><td>The Tier 3 SME creates a Problem Ticket in ServiceNow to capture the increase of tickets / trend analysis, links all pertinent incidents to it, and informs Tier 1 Leadership of the Problem Ticket. Continue to Step 16.</td></tr><tr><td>The issue will only affect one or a few users</td><td>Continue to Step 16.</td></tr></table>	If...	Then...	<u>Three or more Incident tickets are created</u> due to end users/customers encountering the same issue or if the incident has the <u>potential to affect multiple users</u>	The Tier 3 SME creates a Problem Ticket in ServiceNow to capture the increase of tickets / trend analysis, links all pertinent incidents to it, and informs Tier 1 Leadership of the Problem Ticket. Continue to Step 16.	The issue will only affect one or a few users	Continue to Step 16.
	If...	Then...					
	<u>Three or more Incident tickets are created</u> due to end users/customers encountering the same issue or if the incident has the <u>potential to affect multiple users</u>	The Tier 3 SME creates a Problem Ticket in ServiceNow to capture the increase of tickets / trend analysis, links all pertinent incidents to it, and informs Tier 1 Leadership of the Problem Ticket. Continue to Step 16.					
The issue will only affect one or a few users	Continue to Step 16.						
16.	The Tier 3 SME assesses, troubleshoots, and resolves the Incident while: <ul style="list-style-type: none">a. Aiding in the troubleshooting and recovery of downed serviceb. Communicating technical findingsc. Helping to identify and engage alternate resource(s), e.g., external vendors, for assistance if necessaryd. Remaining engaged until resolution or until other technical resources take over						

Continued on next page



Redacted

6/6/2023

Process Description, continued

Resolution

Step	Action						
17.	The Requestor (or end user) confirms that the Incident is resolved and service is restored.						
18.	<p>The Incident Owner documents the resolution and how service was restored in [Redacted] and resolves the ticket(s).</p> <p>Note: Depending on the level of escalation, the Incident Owner can be in Tier 1-Tier 3.</p>						
19.	<p>The Incident Owner proceeds based on the chart below:</p> <table><tr><th>If the Incident...</th><th>Then...</th></tr><tr><td>Was Minor</td><td>Stop here.</td></tr><tr><td>Was Major</td><td>The Incident Owner engages Communications to send a [Redacted] Alert notifying the affected parties of service restoration.</td></tr></table>	If the Incident...	Then...	Was Minor	Stop here.	Was Major	The Incident Owner engages Communications to send a [Redacted] Alert notifying the affected parties of service restoration.
If the Incident...	Then...						
Was Minor	Stop here.						
Was Major	The Incident Owner engages Communications to send a [Redacted] Alert notifying the affected parties of service restoration.						

Stop here



Redacted

6/6/2023

Associated Documents

This section provides a list of documents used or referenced in the construction of this document.

Title/Link	Version	Date	Description	Owner
[Redacted] Tier 2 and 3 Support SLA	1.0	2/14/2022	Establishes a collaborative written agreement between [Redacted] and [Redacted].	[Redacted]
Watch Officer Triage Procedure	4.4	7/18/2023	Defines the duties and responsibilities of the [Redacted] Watch Officer.	[Redacted]

Definitions

This section provides the definitions of all abbreviations, acronyms, and terms required to properly interpret this document.

Abbreviation/Term/Acronym	Definition
CI (Configuration Item)	A component of an information system in the CMDB. Can be any IT component, including software, hardware, documentation, personnel, or any combination of them.
Incident	Unplanned interruption to or reduction in quality of an IT Service, or the failure of a Configuration Item (CI) that has not yet affected a service.
[Redacted] Watch Officer	The primary Point of Contact (POC) for all incidents that occur after normal business hours.
Major Incident	Site, multi-site, region, or company-wide major production or critical system outages. A team, group, or department-wide partial outage or degradation of services is also considered a Major Incident. Example: All [Redacted] Staff and Contractors can't access emails.
Minor Incident	An issue with the production environment that may or may not prevent a small number of staff from completing work. Example: A small team of users can't access a secondary website.

Continued on next page



Redacted

6/6/2023

Definitions, continued

Abbreviation/Term/Acronym	Definition
OLA (Operational Level Agreement)	Commitment between internal groups within an organization in support of an SLA (Service Level Agreement). It describes the responsibilities of each internal support group toward other support groups, including the process and timeframe for delivery of their services.
Outage	Time period during which a system fails to provide or perform its primary function.
SLA (Service Level Agreement)	Commitment between a service provider and a client in which particular aspects of the service – quality, availability, responsibilities – are agreed upon.
Service Request	Formal request from a user for something to be provided, for example, a request for information or advice; to reset a password; or to install a workstation for a new user.
Service Restoration	Renewed availability of a service or resource (application, database, server, telephone, network, etc.).

Contributors to This Document

- [Redacted]
- Karl Levy, Technical Writer



Redacted

6/6/2023

Revision History

Date	Description	Preparer	Version
2/23/2022	Initial Draft	Karl Levy	1.0
Redacted	Redacted	Karl Levy	1.1
Redacted	Redacted	Karl Levy	1.2
Redacted	Redacted	Karl Levy	1.3
Redacted	Redacted	Karl Levy	1.4
Redacted	Redacted	Karl Levy	1.5
Redacted	Redacted	Karl Levy	1.6
Redacted	Redacted	Karl Levy	1.7
6/6/2023	Redacted	Karl Levy	1.8

Record of Approvals

Name	Position	Date	Version
Redacted	Redacted	Redacted	1.3
Redacted	Redacted	Redacted	1.5
Redacted	Redacted	Redacted	1.7
Redacted	Redacted	6/6/2023	1.8