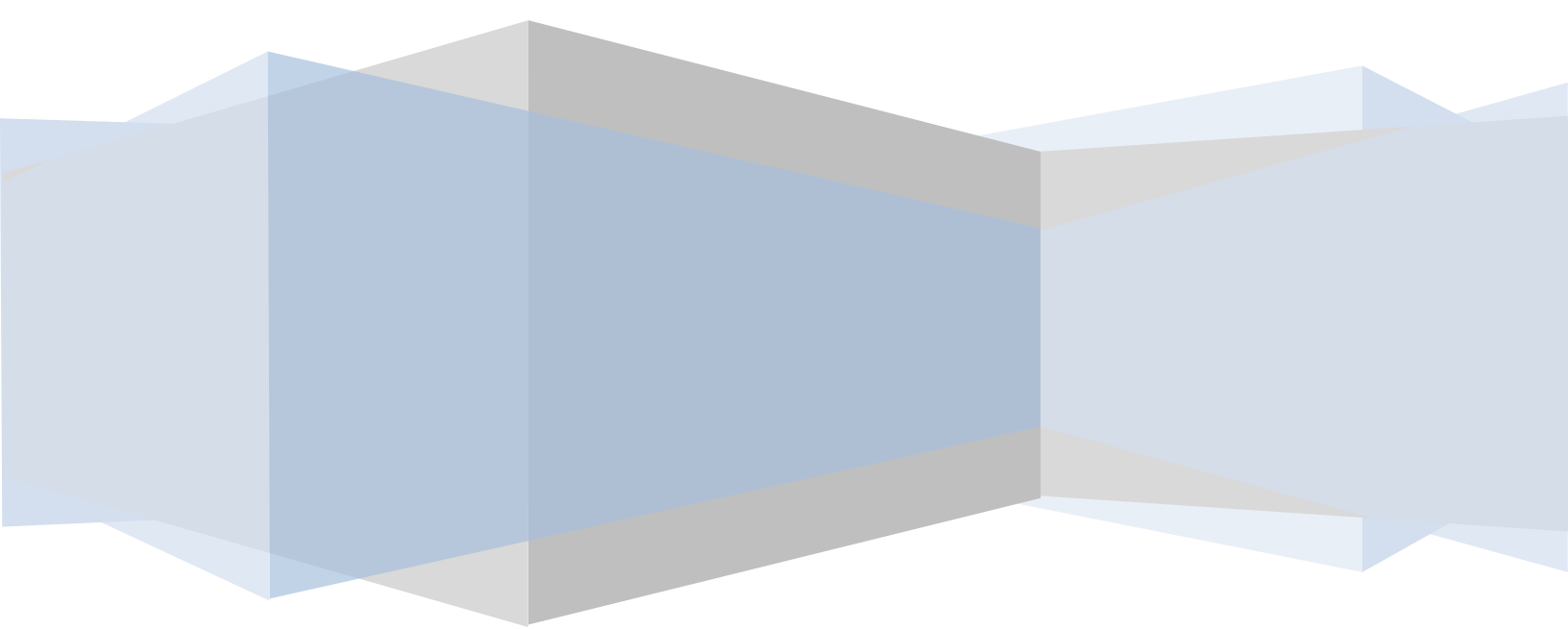


Incident Management Process

Vanderbilt University

October 2020



CONTENTS

Version History.....	3
Introduction	4
Goals, Objectives & Scope	5
goals.....	5
Objectives	5
Scope	6
Process Flow.....	7
Incident & Request Process.....	7
Roles & Responsibilities	10
Incident Roles & responsibilities.....	10
Requester/Customer.....	10
First Line / Service Desk	10
Second / Third Line.....	11
Incident Manager	11
Policies	12
Major Incidents	14
Categorizing Incidents.....	15
Incident Status	16
Notification Triggers	17
Priorities & Service Level Objectives.....	18
Impact, Urgency and Priority.....	18
Service Level Objectives	19
Hierarchical Escalations.....	19
Key Performance Indicators.....	21

VERSION HISTORY

Date	Who	Comments
2/1/17	Reg Lo & Valerie Arraj	First draft
2/22/17	George Anglin	Combine comments & revisions
6/13/2017	George Anglin	Added Break/Fix information, minor updates and clarifications throughout
10/16/2018	George Anglin	Minor corrections and updates
10/28/2020	George Anglin	Add link to Major Incident Guidelines
10/28/2020	Taj Wolff	Approval of document

INTRODUCTION

This document describes Incident Management process for Vanderbilt University IT (VUIT). It is based on the Information Technology Infrastructure Library® (ITIL) and adapted to address Vanderbilt University's specific requirements.

This document is divided into the following sections:

Section	Description
Objectives & Scope	Specifies the objectives of the Incident Management process.
Process Flow	Diagrams illustrating the high-level Incident Management process. In particular the following scenarios are covered: <ul style="list-style-type: none"> • Standard Incident process • Major Incident procedure
Roles & Responsibilities	Identifies the roles within the Incident Management process and the responsibilities for each role.
Policies	Policies that support the Incident Management process
Categorizing Incidents	Two-tiered structure for categorizing Incidents.
Incident Status	Diagram illustrating the possible statuses of an Incident record, how statuses are allowed to change and what triggers the status to be automatically updated.
Priorities & Service Level Objectives	Describes how Priority will be determined from Impact and Urgency, and the target time, to respond and resolve each level of priority.
Key Performance Indicators	Specifies the metrics for measuring the success of the Incident Management process.
Fields on the Incident Record	Provides field specifications including drop down values for Cherwell.

GOALS, OBJECTIVES & SCOPE

GOALS

The goals of the Incident Management process are:

- To provide a channel for customers to request help for an issue or technical problem.
- To provide a channel for monitoring systems to automatically open Incidents in the tool and alert the appropriate technical teams.
- To track Major Incidents.
- To track and monitor SLAs.

OBJECTIVES

An Incident is an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure of a Configuration Item that has not yet impacted an IT service. The purpose of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained.

The specific objectives of Incident Management are:

1. Adopt a single Incident Management process for the entire IT organization.
2. Report on valuable metrics to evaluate effectiveness and efficiency of the process.
3. Base the process on industry standards while addressing customer requirements.
4. Improve communications to users, customers and between IT teams during Incident Management.
5. Consolidate on a single tool including a single customer portal.
6. Use Incident Management to provide input into the Problem Management and Knowledge Management processes.

SCOPE

All incidents related to university owned CIs or assets are in scope. Shared services will continue to be tracked in Pegasus until the service is no longer shared.

The Incident Process owner will own:

- The process of creating/approving requests for new fields/forms in the tool.

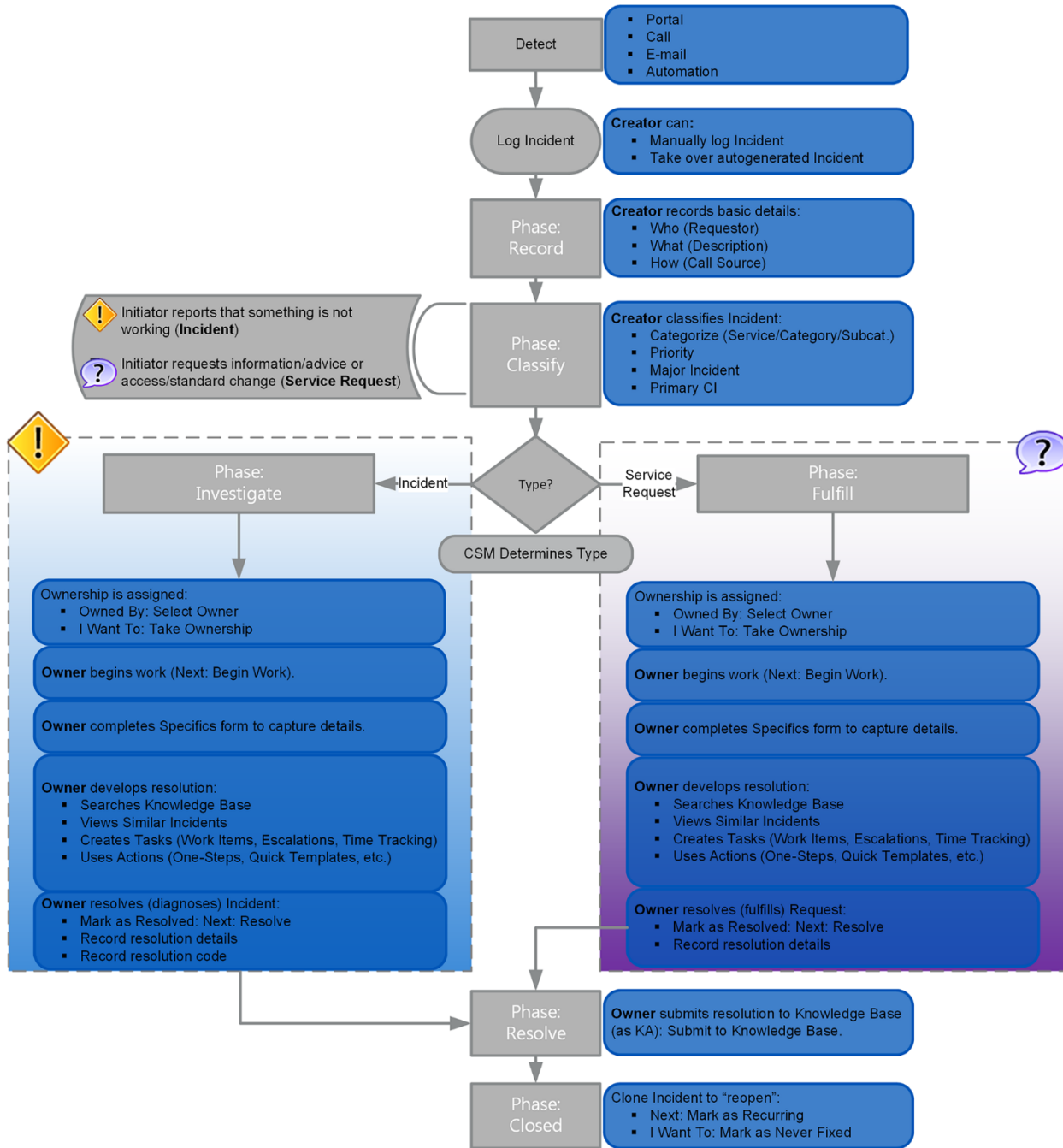
PROCESS FLOW

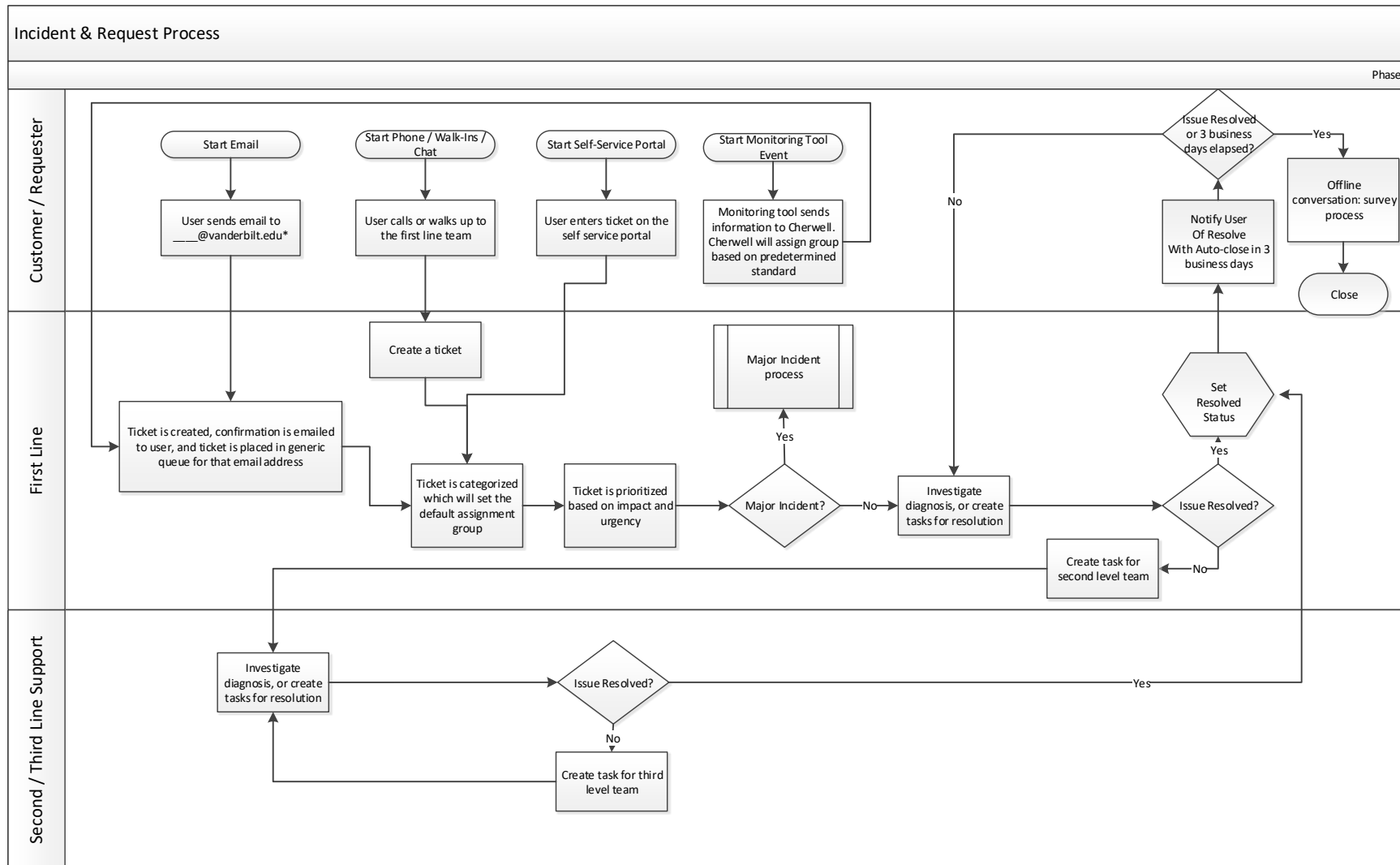
The following page illustrates the Incident Management Process. Major Incidents please refer to the [Major Incident Guidelines](#).

The process flows use “swim-lane diagrams” to illustrate which role is responsible for the activity. These roles are described in more detail in the following section titled “Roles and Responsibilities”.

INCIDENT & REQUEST PROCESS

The workflow diagrams represent the VUIT Incident Management process.





*_@vanderbilt.edu signifies an email address that represents the assignment team for a first line support group.

ROLES & RESPONSIBILITIES

INCIDENT ROLES & RESPONSIBILITIES

REQUESTER/CUSTOMER

1. To request support, submit a help request to [Help IT](#), call (615) 343-9999, email it@vanderbilt.edu or visit the [VUIT web page](#) for more information.
2. If it is an urgent issue, call (do not use email or the self-service portal). When calling about the issue, please explain why this is urgent. You must be available to collaborate on resolving urgent issues.
3. When completing the description of the issue in the portal or when sending an email requesting support, be as descriptive as possible, e.g. describe the screen you are on, the error message you see, the steps you performed just prior to the issue, etc.

FIRST LINE / SERVICE DESK

1. When recording an Incident, be as descriptive as possible.
2. Before escalating the Incident, make sure you searched for and applied the relevant Standard Operating Procedures (SOPs) and Knowledge articles.
3. If you notice that the Incident is categorized incorrectly, correct the category.
4. Record any activity performed in the Journal tab.
5. Assign a task to the appropriate second or third line support group to escalate.
6. When resolving an Incident, be as descriptive as possible when completing the closing notes, i.e. describe what you did as opposed to entering “done” and “fixed”.
7. If this Incident is the same as another Incident - link the Incidents.
8. If this Incident record is a candidate for a Knowledge Article, propose that the Incident record should become a Knowledge article.
9. If this Incident was caused by a Change, link the Incident to the Change.

10. Incoming emails - where the "From" email address does not match a customer record in the system – will have a default user assigned to the Incident. First line will triage as necessary.

SECOND / THIRD LINE

1. If the customer contacts you directly, encourage good behavior, i.e. use official entry points into first line.
2. If you notice that the Incident is incorrectly categorized or misassigned, correct the category or assignment.
3. Record any activity performed in Journal tab.
4. If further assignment is necessary, create another task for the appropriate support group.
5. If an Incident(s) is/are associated with a Major Incident, link the Incident to the Major Incident.
6. If an Incident record is a candidate for a Knowledge Article, propose that the Incident record should become a Knowledge article.
7. If an Incident(s) was/were caused by a Change, link the Incident to the Change.

INCIDENT MANAGER

The Incident Manager is the single individual responsible for the Incident Management process across all of IT. Their responsibilities include:

1. Ensures that all of IT follows the Incident Management process.
2. Analyze Incident metrics.
3. Sponsor improvements to the process or tool(s).

POLICIES

1. All VU Incidents and Requests must be recorded in Cherwell. The contact details of anyone with a VUNetID will be captured in the Customer fields. For all other customers contacting first line support, a generic Default Customer account will be used.
2. If a customer is requesting support or service on behalf of another individual, the “Requested For” fields will be used to indicate the details of the individual who is the target of the service being provided. First line support should indicate which individual(s) should receive communication as the Incident is being moved through the process to resolution.
3. First and second line support will maintain a status indicator on the contact record in Cherwell to signify that an individual is a VIP.
4. If a customer emails, chats or calls a second or third level support analyst to start an Incident, the second or third level support analyst should encourage the customer to start at the appropriate first line support team.
5. The urgent flag on an email does not affect the priority of an Incident. If the Incident is urgent, customers should follow up with a phone call.
6. Whoever receives the Incident first must ensure that the description is detailed enough so that subsequent levels of support can work on the Incident without needing to contact the first person who received the Incident.
7. Any work conducted on an Incident must be recorded in the Journal tab of the ticket.
8. An Incident can only be put on-hold (taken off the Service Level Agreement clock) for the following reasons:

- | | |
|--|--|
| • Customer is unavailable | • Issue requires additional research |
| • Need is for a future date/time | • Pending 3 rd Party Vendor |
| • Pending Approval (Finance or Management) | • Pending Change Request |
| • Pending Completion of Tasks | • Waiting for non-capital h/w |
| • Waiting for response | |

9. If the support analyst realizes the Incident they just created is the same as another open Incident (possibly from another customer), they should link the new Incident (child) to the existing Incident (parent). When the parent is resolved, the analyst will have the option to automatically resolve child tickets.
10. If the support analyst discovers that the Incident was caused by a Change, they must link the Incident to the appropriate Change record.
11. The “Close Notes” must describe what was done to resolve the Incident. “Fixed” or “Done” is not sufficient.
12. A “Cause Code” must be used to indicate a reportable cause for an Incident.
13. SECURITY RELATED INCIDENTS: If the Incident is assigned to the Security Incident Response (SIR) team, only the SIR team can have visibility to the ticket. If another team needs to work the ticket, the SIR team will create a task and assign it to the team from which they seek assistance.
14. BREAK/FIX INCIDENTS: If the Incident requires an analyst to perform a restore or restart of a system or service to strictly restore a system back to normal state only (NO CHANGES), this would be documented in an Incident ticket. If any form of change is involved, then an Emergency change would be opened.
15. After an Incident is resolved, the customer has 3 business days to indicate that the Incident was not resolved to their satisfaction, otherwise the Incident will automatically close.
16. For customer-reported Incidents, the Incident Owner (typically first line support) will close the loop with the customer during resolution.
17. For VUIT-reported Incidents, the Incident Owner will close the loop with the VUIT requester.

MAJOR INCIDENTS

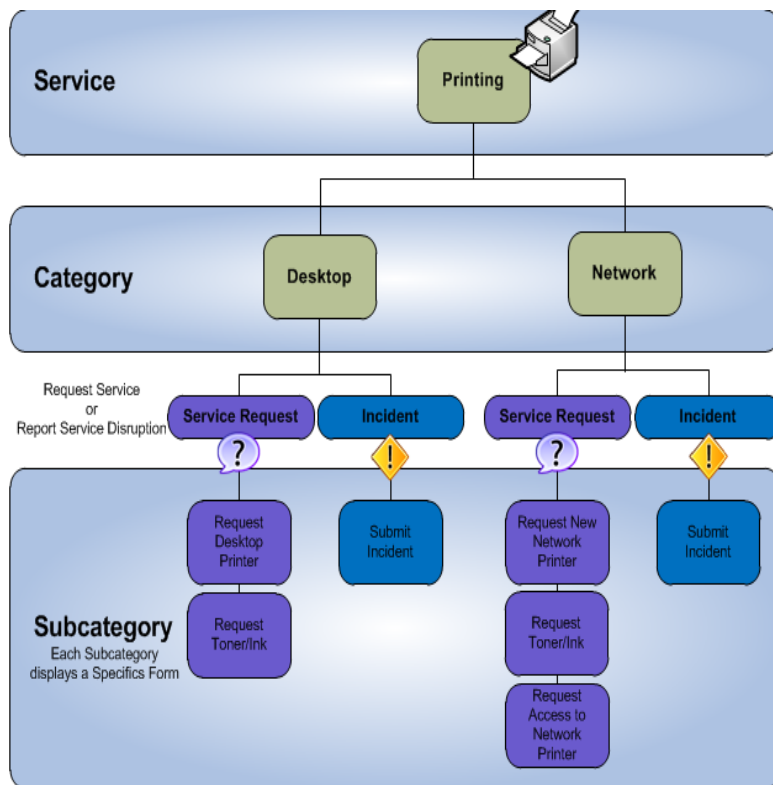
Refer to the [Major Incident Guidelines](#) document.

CATEGORIZING INCIDENTS

Incidents will be categorized according to the Service, Category, and Subcategory Scheme available in Cherwell.

- Service = EDUCAUSE model “service offering”
- Category = Component of the service offering
- Subcategory
 - Drives ticket differentiation (Request vs Incident)
 - Is more aligned with an “action”

These values are service-dependent and are not listed in this document. However, the structure for this construct is represented in the diagram below:



INCIDENT STATUS

The following are the possible statuses of an Incident record and how they may flow:

1. **New:** Incident/Request is being created, recorded (initial details), classified, and assigned to a team.
2. **Assigned:** Incident/Request has been assigned to a technician.
3. **In Progress:** Incident/Request is being investigated/fulfilled and resolved by an owner.
4. **Pending:** Incident/Request is temporarily paused (Stop the SLA clock).
5. **Resolved:** Incident/Request has been resolved and is waiting to be closed.
6. **Closed:** Incident/Request is closed.
7. **Reopened:** Incident/Request is reopened because the issue was not fixed or reoccurred.

The following shows the valid progression from one status to another. The leftmost column shows *current state value*. The top row shows *target state value*. Where the intersection of the two is shaded light gray, the progression from current state to target state is valid and allowed. Where the intersection of the two is shaded dark gray, the progression from the current state to the target state is not allowed. The progression to close is universally allowed as a mechanism for a requester/end user to “close” an Incident when it has resolved itself or if the customer has found a solution and remediation is no longer necessary.

	New	Assigned	In Progress	Pending	Resolved	Closed	Reopened
New							
Assigned							
In Progress							
Pending							
Resolved							
Closed							
Reopened							

NOTIFICATION TRIGGERS

State changes will trigger an email notification as follows:

State	Recipient
New	Requester – Inform that ticket has been created and provide ticket number.
Assigned (Incident or Task)	Owner - Inform that ticket has been assigned to them and provide ticket number. Urgent priority tickets will send notice to xMatters via REST API. xMatters will notify teams.
In Progress	Owner - Remind him/her that the Incident has been inactive for three days.
Pending	Owner – Remind him/her to take action on the Incident at the end of the Pending period.
Resolved	Requester – Inform that issue is resolved and requester has 3 days to respond that the issue has not been resolved to their satisfaction.
Reopened	Owner – Inform that ticket has been reopened for further corrective action.
Closed	Requester - Customer Survey e-mail (rules TBD)

PRIORITIES & SERVICE LEVEL OBJECTIVES

IMPACT, URGENCY AND PRIORITY

Priority is determined by the support analyst (not the customer) by first determining the Impact and Urgency.

		Impact		
		<i>University-wide</i>	<i>Small Group</i>	<i>Individual</i>
Urgency	<i>Work is blocked</i>	Urgent	Urgent	High
	<i>Work is degraded or potentially degraded</i>	Urgent	High	Normal
	<i>Work is unaffected</i>	Normal	Low	Low

VIPs will automatically get a priority of Urgent. The first-line analyst can change the priority if the VIP indicates that the Incident is not Urgent.

SERVICE LEVEL OBJECTIVES

The Service Level Agreement (SLA) is dependent on the Priority.

Priority	Time to Respond	Time to Resolve
Priority Urgent (1)	.5 hours (contact) (24/7)	4 hours (24/7)
Priority High (2)*	2 hours	12 hours
Priority Normal (3)	4 business hours	24 business hours
Priority Low (4)	8 business hours	48 business hours

HIERARCHICAL ESCALATIONS

Hierarchical escalations are used when a Level 1, 2, or 3 technician does not or cannot respond or resolve within a defined timeframe for a specified priority of Incident. These notices are delivered to team managers so they can manage work speed and communication to the end user/requester or other key stakeholders as necessary.

Time to respond is the time between the ticket being created and the ticket being put into the “In Progress” status.

Priority	Time to Respond	Hierarchical Escalation on Response SLA/O	Time to Resolve	Hierarchical Escalation on Resolution SLA/O
Priority Urgent (1)	.5 hours	xMatters handles escalations. When you accept in xMatters, xMatters will set the status of Cherwell Incident to "In Progress" and the owner	4 hours	At 100% email assignment group manager
Priority High (2)	2 business hours	At 100%, i.e. 2 hours, email to assigned group manager	12 business hours	At 75% or 8hrs email assigned to person At 100% email assigned group manager
Priority Normal (3)	4 business hours	At 100%, i.e. 4 hours, email to assigned group manager	24 business hours	At 75% or 16hrs email assigned to person At 100% email assigned group manager
Priority Low (4)	8 business hours		48 business hours	

KEY PERFORMANCE INDICATORS

VUIT will focus on a few select Key Performance Indicators (KPIs) to measure the success and efficiency of the Incident Management process. As the Incident Management process matures, the KPIs may change to focus on different areas that need improvement.

1. Total number of Incidents by Team.
2. Number and percentage of Incidents closed by first line.
 - First call resolution is 4 or fewer saves between New to Resolved.
3. Number of open Incidents and Tasks by Team
4. Number and percentage of Incidents that were re-opened by category, support group, support analyst, etc.