# VUIT
# Incident Management Process

# Goals

The goals of Incident Management at VUIT are:

1. To provide a channel for customers to provide a method to request help for an issue or technical problem.
2. To provide a channel for monitoring systems to automatically open Incidents in the tool and alert the appropriate technical teams.
3. To track issues and group common issues as a Major Incident.
4. To track and monitor SLAs.

# Definition

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.

# Break/Fix vs. Emergency Change

## Break/Fix

**IF…**
- University only services/customers affected.
- Break/fix restore to a normal state (restart or reboot only, no changes).

**THEN…**
1. Open Incident ticket in **Cherwell**, if one has not already been opened via FireScope. An Incident is required for restarting or rebooting a system or service.
2. Notify NOC at 322-2954 or Skype of Incident ticket, situation and how/when you will be resolving it.
3. NOC will escalate system alerts if necessary.
4. NOC will send VUIT notification, upon Tech request, stating the issue, server name(s), Service affected, Incident # and what was being done.

**IF…**
- **Shared** services/customers affected.

**THEN…**
1. See **Pegasus** Emergency process.

# Break/Fix vs. Emergency Change

## EMERGENCY

**IF…**
- **University only** services/customers affected.
- Break/fix change to restore to normal state.

**THEN…**
1. Open Incident ticket in **Cherwell.**
2. Obtain verbal or written approval from manager/director
3. Notify NOC at 322-2954 or Skype of Incident ticket, situation and how/when you will be resolving it.
4. Upon completion and verification of Emergency change, open change ticket in Cherwell documenting the change you implemented and link it to your incident ticket. Include your manager/director approval.
5. Change will be reviewed at next available VUIT CAB meeting.

**IF…**
- **Shared** services/customers affected.
- Preventing or recovering from an outage.

**THEN…**
1. Open Incident ticket in **Pegasus** (if one isn't already open).
2. Open an Emergency change in **Pegasus**, referencing your Pegasus incident ticket.
3. Obtain director approval.
4. Move change to 'Ready for CAB' phase. xMatters will notify MCIT Change Management team.
5. Change Management team will go seek AOC approval and once approved, will move change to Implementation Pending.
6. Notify NOC at 322-2954 or Skype of Incident ticket, situation and answer any questions.
7. NOC will sent out VUIT Alert communication to MCIT Datacenter DL and VUIT DL.
8. Implement Emergency change only the tasks above have been completed.

# Incident Roles & Responsibilities

Requestor/Customer

- To request support, use the self-service portal or email or call your area's Support Desk (Tech Hub, VMDP, DTS).
- 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.
- When completing the description of the issue in the portal or when sending an email requesting support, be as descriptive a possible, e.g. describe the screen you are on, the error message you see, the steps you performed just prior to the issue, etc.

# Incident Roles & Responsibilities

First Line/Service Desk

- When recording an Incident, be as descriptive as possible.
- Before escalating the Incident, make sure you searched for and applied the relevant Standard Operating Procedures (SOPs) and knowledge articles.
- If you notice that the Incident is categorized incorrectly, correct the category.
- Record any activity performed in the Notes field or Journal tab.
- Assign a task to the appropriate second or third line support group to escalate.
- 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”.
- If this Incident is the same as another Incident - link the Incidents.
- If this Incident record is a candidate for a Knowledge Article, propose that the Incident record should become a knowledge article (available in Phase 3).
- If this Incident was caused by a Change, link the Incident to the Change.
- 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.

# Incident Roles & Responsibilities

## Second/Third Line

- If the customer contacts you directly, encourage good behavior, i.e. use official entry points into first line.
- If you notice that the Incident is wrongly categorized or misassigned, correct the category or assignment.
- Record any activity performed in the Notes field or Journal tab.
- If further assignment is necessary, create another task for the appropriate support group.
- If this Incident is associated with a Major Incident, link the Incident to the Major Incident.
- If this Incident record is a candidate for a Knowledge Article, propose that the Incident record should become a knowledge article (available in Phase 3).
- If this Incident was caused by a Change, link the Incident to the Change.

# Incident Roles & Responsibilities

## Incident Manager

- Ensures that all of IT follows the Incident Management process.
- Analyze Incident metrics.
- 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 Requester fields. For all other customers contacting first line support, a generic Guest account will be used.
2. If a customer is requesting support or service on behalf of another individual, the “requested on behalf of” field will be used to indicate the details of the individual who is the target of the service being provided, as well as the individual making the request (requester). 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.

# Policies

7. Any work conducted on an Incident must be recorded in the Notes field or 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:

| Waiting for customer: | Waiting for more information from customer |
|---|---|
| On-Hold – Waiting for Vendor: | Waiting for a supplier |
| On-Hold – Scheduled Work: | Work has been scheduled, e.g. desktop technician will visit customer at an agreed date/time |

9. If the support analyst realizes the Incident they just created is the same as another open Incident (possibly from another customer), they must link the new Incident (child) to the existing Incident (parent). Any changes to the parent's status, category, or assignment will automatically update all child incidents, e.g. if the parent is resolved, all children are automatically resolved.
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.

# Policies

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. The priority of the Incident ticket must be copied to the associated task. Tasks marked as Urgent as a result of their associated Incident ticket should page the assignment team. The notification of a task assignment should clearly note that the Task is associated with an Incident.
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, relative to the customer's time zone, 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 is the team that will close the loop with the VUIT requestor.

# Incident Status

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

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

# 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) |

# Impact, Urgency and Priority

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

| | | Impact | | |
|---|---|---|---|---|
| | | University-wide | Small Group | Individual |
| Urgency | Work is blocked | Urgent | Urgent | High |
| | Work is degraded or potentially degraded | Urgent | High | Normal |
| | Work is unaffected | Normal | Low | Low |

# Impact, Urgency and Priority

* An Incident where the condition for urgency is “Work is blocked” and Impact is “University-Wide” should be considered as a candidate for Major Incident, but a Major Incident is a declared state determined by the situation at hand.

* 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.

# SLA Response Time

The Service Level Agreements (SLAs) 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 |

# Escalations

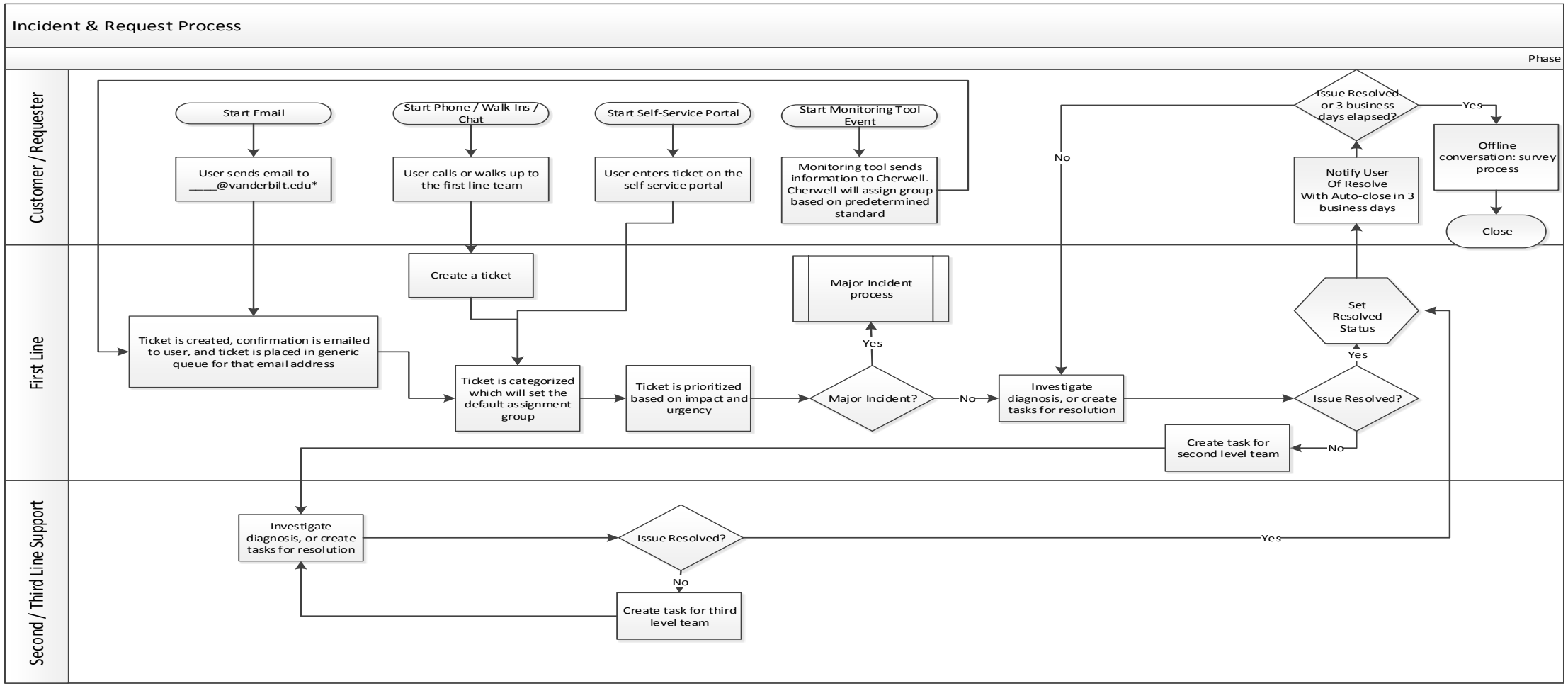
- Hierarchical escalations are used when a Level 1, 2, or 3 technician does not or cannot respond or resolve within a defined timeframe for a specified priority of Incident. These notices are delivered to team managers so they can manage work speed and communication to the end user/requester or other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

# Escalations

| 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<br>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<br>At 100% email assigned group manager |
| Priority Low (4) | 8 business hours | | 48 business hours | |

# Process Flow



# 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 category, priority, support group, support analyst, etc.
2. Mean time to Repair (MTTR) an Incident by category, priority, support group, support analyst, etc.
3. Number and percentage of Incidents closed by first line.
    - First call resolution is 30 minutes between new to resolved, without re-assign, and without dispatch flag set.
4. Number of active Incidents and Tasks by category, priority, support group, support analyst, etc.
5. Number and percentage of Incidents that were resolved within the SLA/O (or due date) by category, priority, support group, support analyst, etc.
6. Number of Incidents that were caused by Changes.
7. Number and percentage of Incidents that were re-opened by category, support group, support analyst, etc.

# ANY QUESTIONS?