Incident Management Policy	
Policy #	Effective Date: 3/31/2021
Version 3.0	Responsible Party: Albert Strong

Revision History

Rev	Date	Description	Author(s)
1.0	8/1/2020		Albert Strong
2.0	8/7/2020	Additional content, Key Control List	Albert Strong
3.0	3/31/2021	Review	Albert Strong

Table of Contents

1.1 Introduction

An incident is an unexpected disruption to a service. It disturbs the normal operation thus affecting end user's productivity. An Incident may be caused due to an asset that is not functioning properly or network failure.

1.2 Incident vs service request

A service request is 'a formal request from a user for something to be provided – for example, a request for information or advice. This policy refers to procedures required for an incident only.

1.3 Security Incident or "Breach"

A security breach is any incident that results in unauthorized access of PRIVO data, applications, services, and/or networks by bypassing our underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters our private, confidential or unauthorized logical IT perimeter. A security incident may require special customer notification and other procedures. **Please refer to the Security Incident and Breach Notification Policy for the policy and procedures regarding a security incident.**

1.4 Security Incident Management

For purposes of incident management, a security incident will follow the steps outlined herein.

1.5 Audience

This process applies to all permanent and temporary staff within UPLEVEL who directly work on production infrastructure, along with staff responsible for infrastructure supporting the delivery of UPLEVEL services. This process equally applies to contractors and visitors who work for and / or visit the company.

1.6 Owner/Location

Ownership of Processes and Procedures in support of UPLEVEL Incident Management Policy reside with the executive and security teams. .

2 Incident Management Process

The UPLEVEL Incident Management Process document defines Incident Management processes which will underpin the support of the Incident Management Policy. Processes defined within this document are processes which are common across Network Operations teams, working across all divisions. Scope

The UPLEVEL Incident Management Process defines process and procedure in relation to Incident Management, which should be undertaken by all relevant teams. . This process document defines process and procedure for Incident Management activities which should provide the minimum amount of activity for any given incident.

This document will only address process and procedure which is common across all teams.

2.1 Incident Identification

Incidents are identified by UPLEVEL's cloud provider event management systems and presented to the relevant team member with responsibility for the monitoring, management and availability of the service. Incidents can and will also be identified by other UPLEVEL internal organizations or by customers calling UPLEVEL.

2.2 Incident Tracking

Relevant incidents or service requests managed by the UPLEVEL Engineering team requires a Jira ticket to be opened for tracking.

Tickets are created for incidents that have been identified by UPLEVEL *and* or as a result of a UPLEVEL customer contacting the team.

2.3 Incident Categorization

Incidents should be categorized within the Jira ticketing system by appropriately populating the required " fields. It is important all information is accurate, and documented within the ticket by to allow for correct ownership and management of the incident and accurate reporting.

2.4 Incident Prioritization

Prioritization of any incident is determined by a combination of impact and urgency as selected when creating the incident ticket. When an incident is reactively reported, the urgency and particularly the Impact/Risk should be established in conjunction with the customer and the impact they are experiencing.

2.4.1 Impact

Impact is defined as the effect the outage is having on the customer(s) and their ability to use the service. Impact is rated by blocker, critical, high medium, or low.

2.4.2 Urgency

Urgency is defined by how quickly the business or customer requires a resolution and the level of risk to the business or customer. Urgency is rated by blocker, critical, High, Medium, or Low.

2.4.3 Priority

Ticket priority is automatically assigned based on the selected impact and urgency rules defined within the Jira ticketing system. Ticket priority will range from whether the incident is blocker, critical, high, medium or low. Appropriate ticket priority is very important because the priority will determine the technical and management escalation guidelines, as well as the communication requirements.

Target Response Time is defined as the time from the onset of the service incident to the incident ticket being opened and investigation of the incident started.

2.5 Major Incident Identification

Service incidents which result in an incident ticket being opened as a blocker, or critical will invoke the Business Continuity Plan or the Disaster Recovery Plan . Please refer to the Business Continuity Plan or the Disaster Recovery Plan for further information and procedures.

2.6 Initial Diagnosis

During the initial stages of diagnosis, check recent change management records to confirm that a known change didn't inadvertently impact the customer. Additional correlation should also be undertaken with any ongoing major issues that the incident could potentially be related to.

2.7 Customer Notifications & Ticket Updates

For service impacting incidents detected by UPLEVEL, a customer notification must be made upon initial creation of an incident ticket if applicable. Maintaining effective customer communications is an important part of incident management and must be maintained through to incident resolution.

All open tickets should be reviewed and updated at standard defined intervals by the individual the ticket is assigned to, unless alternate update intervals have been agreed with the customer or the next action date indicates otherwise.

The time field should be used as a prompt for next actions regardless of whether this is a technical action or a customer update action. Individual responsible reviews the time field.

2.8 Investigation and Troubleshooting

Investigation and diagnosis should include a variety of activities such as :Establishing what has gone wrong or what is being sought by the customer

- Confirming and logging the time the incident occurred and the chronological order of events
- Confirming the full impact and scope of the incident
- Identifying any events which could have triggered the incident
- Reviewing previous Jira tickets to determine if this is a repeat incident
- Initial steps to troubleshoot and restore impacted services
- Engagement of 3rd parties where relevant and required

NOTE: Initial efforts for any service incident should be restoration of service, mitigation against further service impact, followed by root cause analysis and remediation. Under no circumstances should a service be left failing or impaired whilst the root cause of the fault is investigated and understood.

2.9 Technical & Hierarchical Escalation

2.9.1 Technical Escalation (Functional)

If the diagnosis, investigation and troubleshooting process has failed to resolve service within the ticket timeframes, an escalation should occur to engage additional technical resources. Technical escalations should proceed until the appropriate technical resources are engaged to adequately evaluate and troubleshoot the incident.

2.9.2 Hierarchical Escalation (Management)

If an incident has met criteria for a management escalation, the team should initiate a management escalation. Management escalations should proceed as defined by the severity and duration of the service incident following the below escalation matrix and contact reference.

2.10 Incident Resolution and Recovery

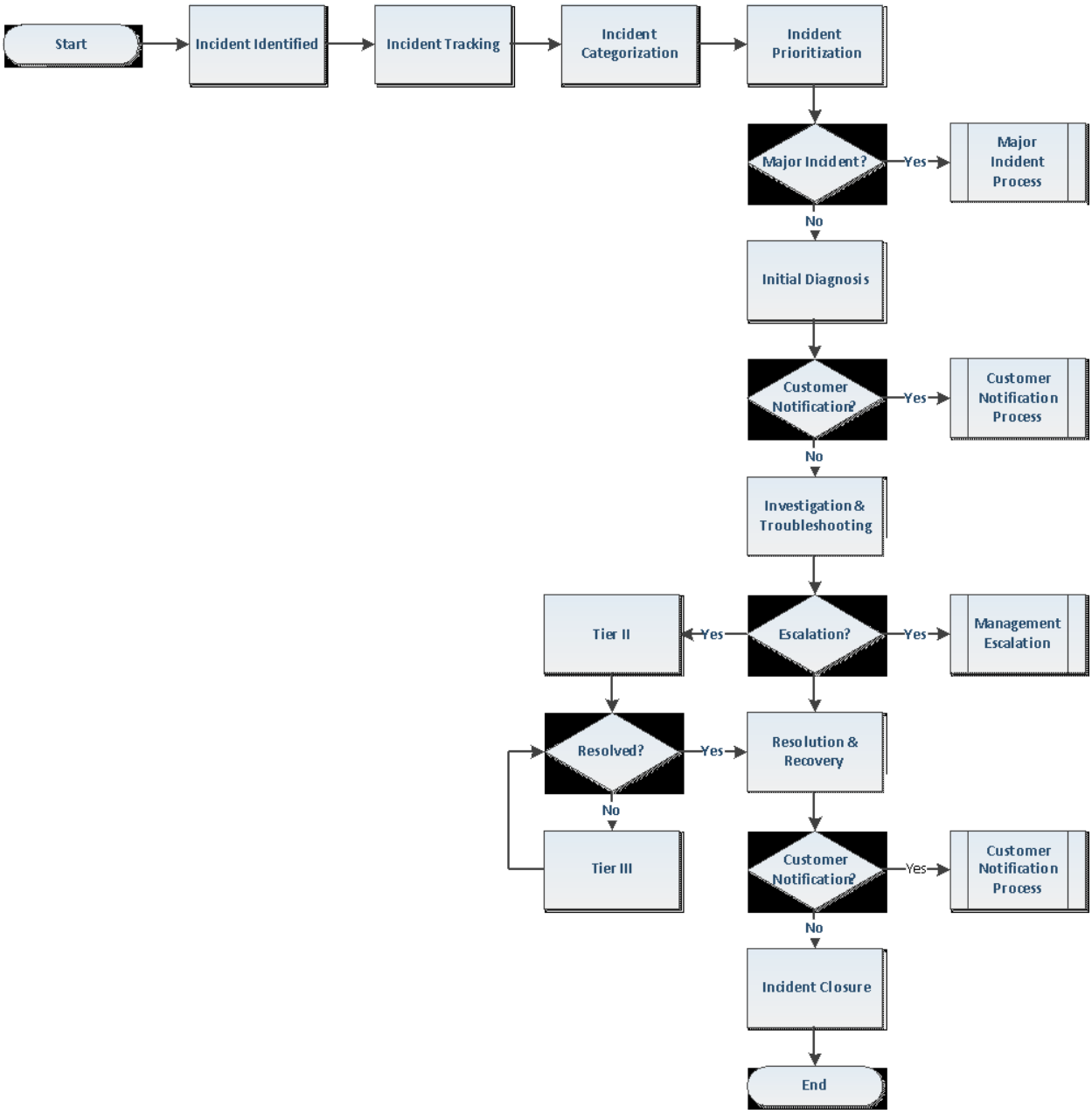
Once the issue has been resolved and normal levels of service have been restored **AND** confirmed by the customer(s) all appropriate information should be documented in the relevant ticket. Confirm with the customer that normal service levels have resumed

- Review ticket information and resolution for accuracy.
- If this is a repeat issue or if there is a risk of the incident occurring again because of a known / unknown underlying cause e a Jira ticket must be created to track the ongoing problem outside of the incident management process and linked to previous related to tickets

2.11 Incident Closure

Once all actions are complete in reference to major incident reviews and production of incident reports and once confirmation has been received from the customer that the incident is fully resolved and with the customers consent, the ticket can be closed.

Incident Management Process Flow



Key Security Controls

- ❑ There is an Incident Management Response Policy and Procedures
- ❑ Our incident response and management policy has been reviewed and updated within the last year
- ❑ An owner is assigned to the incident response policy
- ❑ A process is defined on how employees report incidents internally
- ❑ Employees are formally trained on how to recognize an incident and how to report it during the on-boarding process
- ❑ All incidents are logged in a centralized ticketing system
- ❑ Incidents are classified by their urgency and/or importance and resolved in a timely manner