Policy Title: Information Technology Services – Incident Management

Policy Number:

Established: July 2019

Approved by:

Last Approval Date:

Revision Date:

Position Responsible for Maintaining and Administering the Policy: Executive Director, Information Technology Services

Contact: Ryan Kenney, Executive Director, IT Services, (519) 253-3000 ext. 2740

Table of Contents

Policy Statement

This Policy establishes a defined workflow for response, documentation, and communication of incidents in Information Technology (IT) Services associated with owned and / or managed technology solutions and support services.

Purpose

Information technologies, including those servers, infrastructure, and applications that are supported by IT Services, impact the entire campus. When problems related to these technologies are identified, responsible IT Services staff need to follow established guidelines and protocols for response, documentation, and communication such that the Department can be responsive, resolve issues in a timely manner, involve additional stakeholders (internal and / or external) as may be necessary, and appropriately communicate status and next steps to affected members of the campus community.

Scope

This Policy applies to all information technology related equipment and services that are managed by IT Services, including but not limited to, servers, infrastructure, and applications that are owned by and / or administered by the Department.

Responsibilities:

1. IT Services has the responsibility to:
    - Enforce this Policy and set specific problem management guidelines and protocols related to information technology solutions
    - Ensure that all incident management related actions and communications are provided
2. Client areas have the responsibility to:
    - Be aware of this Policy and take appropriate measures to ensure compliance
3. IT Steering Committee has the responsibility to:
    - Regularly review this Policy
    - Provide feedback and guidance on this Policy
    - Approve amendments to this Policy

Exceptions to Policy

There may be occasions where this Policy cannot be followed to its full extent due to emergency changes that are quick to develop / deploy and must to be introduced as soon as possible in order to restore information technology related services and thus mitigate significant risk to the University.

In the event of this situation, the responsible staff of IT Services will proceed with required actions to restore services and follow up to create an associated incident record after associated services are restored for tracking / reporting purposes.

There may also be situations where the IT Leadership Team may determine that certain situations or circumstances require exceptions to this Policy in order to best serve the interests of the University. Such requests should be communicated in writing to the Executive Director, IT Services and should include the exact nature of the exception and, if appropriate, the time period during which the exception should be granted.

Cross-References

None

Definitions

Incident is an unplanned interruption to a service. Primary goal is to restore service as quickly as possible. *Example: a server crashed causing a disruption in the business.*

Problem is a cause, or potential cause, of one or more incidents. Problems can be raised in response to a single significant incident or multiple similar incidents. They can even be raised without the existence of a corresponding incident. Primary goal is to resolve root cause and identify any temporary workarounds. *Example: a server is running out of resources which is causing intermittent crashes.*

Major Incident Manager is the direct IT Leadership Team Member, or designated staff, who is determined to be the "primary" resource for resolving the issue. In events where there may be multiple primary staff, responsibility may be deferred to Assistant Director(s) and/or Executive Director

Procedures

Procedures for Incident Management identified below follow prescribed ITIL process(es). Each identified step in this process is critical to ensuring the Department can provide appropriate service in the event of a problem situation.

1. Detect the Incident
    - An incident is raised through escalation from the IT Service Desk, identification by other IT Services staff , through proactive alerts from IT Services monitoring tools or from end users indicating a disruption to services

2. Document and Categorize the Incident
    - Every detected incident is required to be documented and appropriately completed in the IT Service Management solution (i.e. Team Dynamix)

3. Prioritize the Incident
    - Prioritizing the incident is done on the basis of impact and urgency. This prioritization will serve as the means of alerting the Department to the severity of the issue.

4. Investigating and Diagnosing the Incident
    - The priority of the incident will determine the required protocol for investigation and diagnosis. The following table will describe these protocols:

Priority	Communication Frequency	Communication Channel	Additional Information
High	Bi-hourly or upon request by staff assigned as "responsible" for Incident	Team Dynamix Major Incident Ticket by staff assigned as "responsible" for Incident, as well as e-mail from Major Incident Manager (i.e. IT Leadership Team member)	Requires identification of Major Incident Manager from the IT Leadership Team or assigned designate. The identified Manager will be responsible for providing ongoing oversight / assistance associated with the incident and regular communication to Senior IT Management. Requires a follow up Major Incident/Problem Review meeting.
Medium	Once daily or upon request by staff assigned as "responsible" for Incident	Team Dynamix Incident Ticket by staff assigned as "responsible" for Incident	Depending on type of indent and known length to resolution, the requirement to update certain problem regularly made be updated at the discretion of the responsible member of the IT Leadership Team
Low	Weekly or upon request by staff assigned as "responsible" for Incident	Team Dynamix Incident Ticket by staff assigned as "responsible" for Incident	Depending on type of incident and known length to resolution, the requirement to update certain problem regularly made be updated at the discretion of the responsible member of the IT Leadership Team

1. Resolve the Incident
- Incidents should be resolved as soon as possible. Some resolutions may require following of prescribed Change Management policies and procedures that properly document steps taken to resolve the incident. These steps should be captured in the associated Incident ticket.

2. Close the Incident
- This step should only occur after the incident has been raised, categorized, prioritized, identified, diagnosed and resolved.

3. Major Incident Review

The Major Incident Review is an activity organized by identified Major Incident Manager to assist with prevention of future incident. During this Review, the responsible team will evaluate the incident, properly document associated activities and identify any necessary next steps. The Major Incident Manager will ensure TDX major incident ticket identifies what was done correctly, incorrectly, future change management activities, and any next steps for circulation with IT Senior Management and any other necessary stakeholders outside of the Department

Review Process for Policy

This Policy will be reviewed at least every three (3) years. There may be certain circumstances that may cause for the review of the Policy prior to that date: changes in legislation that affect the Policy; a specific incident triggers a review of the Policy; there is a request made by Senior Management or the Board of Governors to review the Policy.

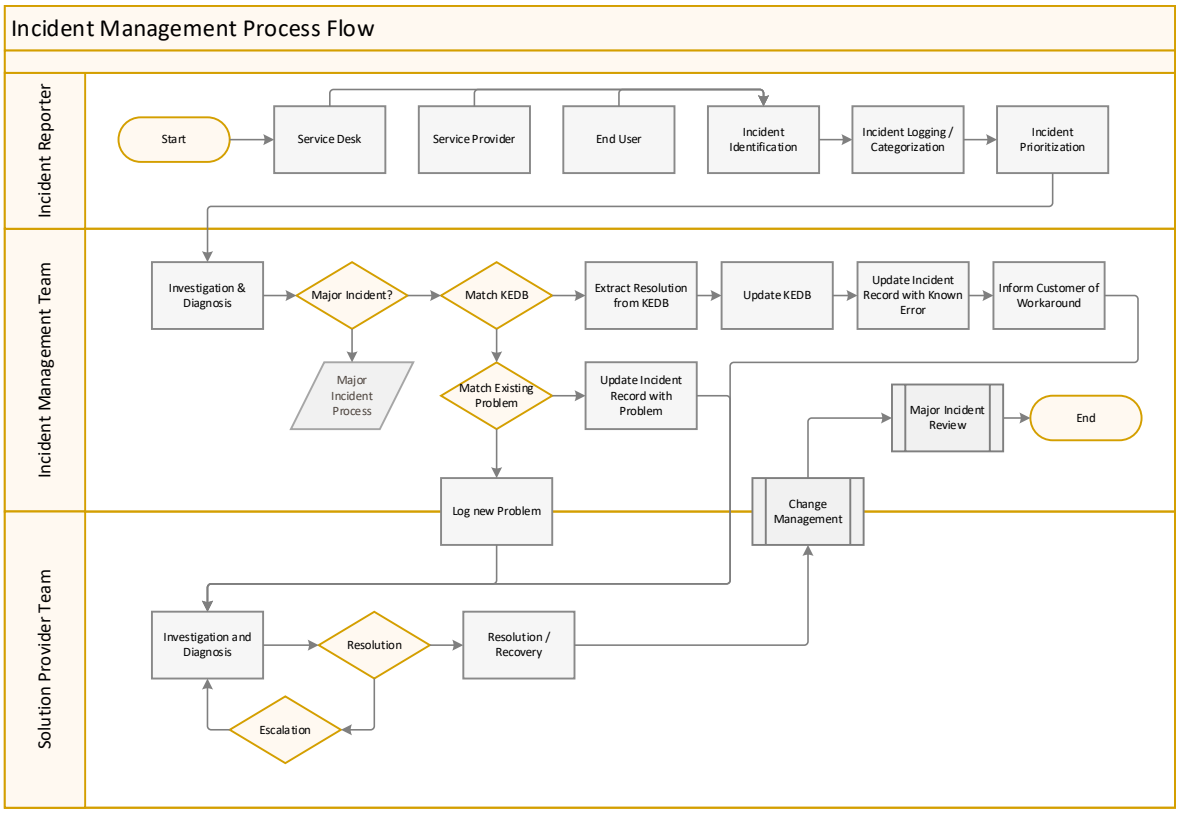
Process for Communicating Policy

The Policy will be posted on the University of Windsor's IT Services website, within two weeks of the approval. Separate notifications may also be sent via e-mail or other means to Departments directly affected by the Policy, or in some cases, the broader campus community if deemed applicable.

Contact Information

Inquiries regarding the policy should be directed to Executive Director, IT Services or appropriate individual in the Department where the Policy was developed, as per the contact information at the introduction of the Policy.

Appendix


Incident Management Process Flow
Incident Reporter
Incident Management Team
Solution Provider Team
Start
Service Desk
Service Provider
End User
Incident Identification
Incident Logging / Categorization
Incident Prioritization
Investigation & Diagnosis
Major Incident?
Match KEDB
Extract Resolution from KEDB
Update KEDB
Update Incident Record with Known Error
Inform Customer of Workaround
Major Incident Process
Match Existing Problem
Update Incident Record with Problem
Major Incident Review
End
Log new Problem
Change Management
Investigation and Diagnosis
Resolution
Resolution / Recovery
Escalation