MacEwan UNIVERSITY | OFFICE OF THE CHIEF INFORMATION OFFICER

IT Incident Management Framework

Standard

Effective Date: September 24, 2015

Authority & Alignment

Authority: D1200 Code of Conduct, D3300 Internal Controls, D8030 Technology Management
Alignment: ITIL V3 Service Operation, Cobit, ISO 20000 Information Technology Service Management

Overview

The primary goal of IT incident management is to restore normal service operation after an incident as quickly as possible and minimize the adverse impact on academic and administrative operations, thus ensuring that the best possible levels of service quality and availability are maintained in support of MacEwan University's (the "University") strategic objectives. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.

The outcome of an IT related incident is an outage or disruption of service. Incidents range from insignificant to potentially catastrophic. Not only do incident outages need to be detected, assessed, responded to, and recovered from as quickly as possible but they must also be categorized, prioritized, and escalated expeditiously so as to proportionally reduce, if not neutralize their negative impact.

Timely and effective response to incidents requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function that ensures incident registration, prioritization, escalation, trend and root cause analysis, and resolution.

Scope and Definitions

This standard applies to any event which disrupts, or which could disrupt, an IT service.

This standard does not apply to service requests.

Definitions[1]:

1. **Incident**. An unplanned interruption to an IT service or reduction in the quality of an IT service.
2. **Incident Management**. Incident Management is the process for dealing with all incidents; this can include failures, questions or queries reported by the users, by technical staff, or automatically detected and reported by event monitoring tools.
3. **Incident Model**. An Incident Model is a way of pre-defining the steps that should be taken to handle a particular type of incident in an agreed way. This will ensure that 'standard' incidents are handled in a predefined way and within pre-defined timescales.
4. **Service Desk**. The Service Desk is the primary point of contact for users when there is a service disruption. The Service Desk provides a point of communication to the users and a point of coordination for several IT groups and processes.

[1] ITIL V3 Service Operation

5. **Service Management**. Service Management is a set of specialized organizational capabilities for providing value to stakeholders in the form of services.
6. **Service Request**. A request from a user for information or advice, a standard change, or access to an IT service.

Compliance & Exceptions

Responsibility for compliance with University policies and standards extends to all members of the University community. Non-compliance may create risk for the University and will be addressed accordingly (see clause 4.5.1 “Respect for the law and University governance” of the University’s policy D1200 Code of Conduct – Employees for additional guidance).

Standard Requirements

1. The Director of IT Infrastructure and Operations is responsible for the requirements of this standard and is accountable to the CIO for the effectiveness of all controls established to fulfill the requirements.
2. ITS will provide sufficient and properly trained resources and appropriate tools to ensure that incidents will be handled within defined timescales.
3. ITS will identify, record and classify incidents, and assign a priority according to process criticality and service level agreements.
    a. It will log all incidents, recording all relevant information so that they can be handled effectively and a full historical record can be maintained.
    b. To enable trend analysis, it will classify incidents by identifying type and category.
    c. It will prioritize incidents based on SLA service definition of process impact and urgency.
4. ITS will define incident classification schemes and models.
    a. It will define incident classification and prioritization schemes and criteria for incident registration to ensure consistent approaches for handling, informing users about and conducting trend analysis.
    b. It will define incident models for known errors to enable efficient and effective resolution.
    c. It will define incident escalation rules and procedures to IT specialist functions.
5. ITS will define a crisis communication procedure for the management of messaging for critical incidents.
6. ITS will provide an awareness program to users on incident reporting.
7. ITS will verify and document satisfactory incident resolution.
8. ITS will establish metrics to judge the efficiency and effectiveness of the incident management process.
9. ITS will regularly track, analyze and report incident trends to provide information for continual improvement.
10. IT Incident Management processes will align with the University's overall incident management system.

Related Content

Type	***Title***
Policy	D8030 Technology Management Policy
Procedure	Incident Management Procedure

Measurement

- ✓ Mean elapsed time to resolve incidents per type and category
- ✓ Number and percent of incidents causing disruption to critical processes
- ✓ Number of incidents open/closed and their risk rankings
- ✓ Number of inaccurate, ineffective, inefficient or misdirected escalations

- ✓ Percent of users satisfied with incident response
- ✓ Percent of incidents resolved within the agreed upon/acceptable period of time

Contact

Director, IT Infrastructure and Operations