Incident Management Procedure

Document ID	**IMP.v.1.0.0**
Effective Date	**2023-04-01**

Table of Contents

1. Purpose and Applicability 3
2. Related Policies and Procedures 3
3. Glossary of Key Terms 4
4. Roles and Responsibilities 5
5. Incident Mangement Overview 6
6. Incident Categorisation and Assessment 8

1. Purpose and Applicability

1.1 The Incident Management Procedure (IMP) outlines the essential requirements in incident handling within the institution: from incident recognition, handling, escalation, to reporting

1.2 The standards and best practices defined within this IMP apply to all units of the institution and are not intended to replace or override any regulatory requirements.

1.3 This IMP will be reviewed on an annual basis or when significant changes occur in regulations, business models, or technologies.

2. Related Policies and Procedures

2.1 This AMP should be reviewed in conjunction with policies and procedures issued by both the organization and the relevant regulatory bodies, which include, but are not limited to, the following:

a. Bank Negara Malaysia (BNM) Policy Document on Risk Management in Technology (RMiT)
b. BNM Policy Document on Business Continuity Management
c. Circulations, notices, and memos issued by BNM
d. Business Continuity Management Policy
e. Risk Management Framework
f. Enterprise Technology Policy
g. Technology Service Management Procedure

3. Glossary of Key Terms

The following are the definition of key terms in this IMP:

Incident refers to an unexpected or unusual event, such as a system failure, that can cause a disruption to the business operations of the institution

Recovery Point Objective (RPO) refers to the maximum acceptable amount of data loss measured in time

Recovery Time Objective (RTO) refers to the maximum acceptable amount of time a system, service, or application can be unavailable after an incident

4. Roles and Responsibilities

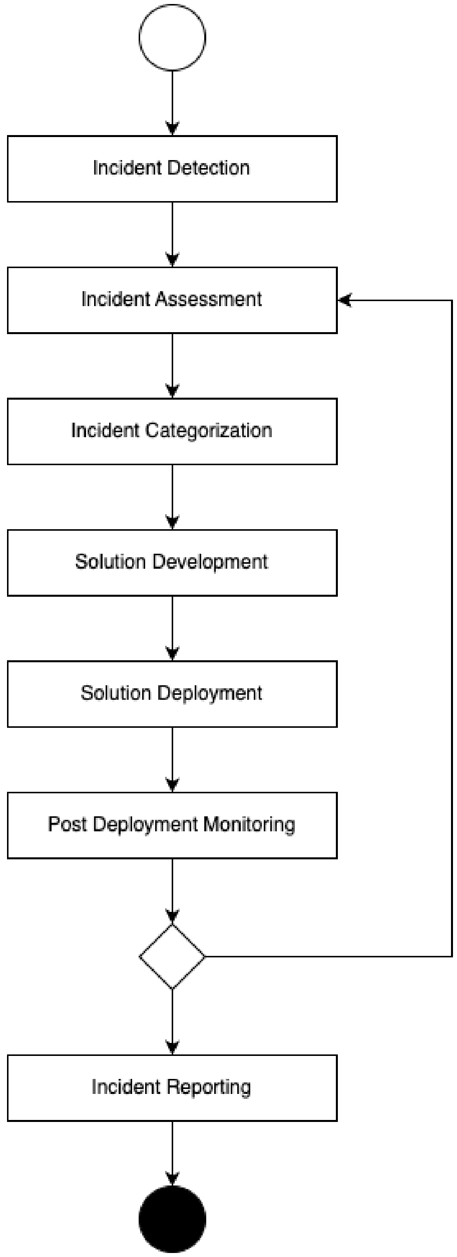
Role	Responsibilities
Incident Manager	• Oversees the entire incident management process, ensuring effective coordination and resolution of incidents • Coordinates response efforts • Communicates with stakeholders • Monitors progress until resolution
Service Desk	• First point of contact for incident reporting. Logs incidents, provides initial support, and escalates if necessary.
Incident Response Team	• A cross-functional team responsible for managing high-priority or critical incidents • Activates during critical incidents • Coordinates with various departments to develop fixes for identified root cause • Ensures rapid resolution
Change Manager	• Ensures that changes arising from incident resolutions are implemented with minimal disruption to ongoing services • Reviews changes related to incidents • Approves or rejects changes • Ensures proper communication of changes

5. Incident Mangement Overview

5.1 The IMP outlines the steps and processes that to identify, respond, resolve, and report all incidents that disrupt the normal business operations of the institutions

5.2 The goal is to restore services and applications as timely as possible while minimizing the impact on business

5.3 The following diagram depicts the overall process for incident handling:



Phase	Details
Incident Detection	• An incident caused by the degradation of one of applications or services is detected through either user reporting or system monitoring
Incident Assessment	• An initial assessment by the respective system owners to determine the severity of the issue and potential root cause
Incident Categorisation	• The incident is categorised according to the incident categorisation and severity matrix describe in Section 6
Solution Development	• Preparation of fixes based on the incident assessment findings • Verification of fixes against identified root cause
Solution Deployment	• Deployment of fixes to target application/system according to the change management procedure
Post Deployment Monitoring	• Monitoring of system health after the deployment of fixes to ensure root cause is addressed • If the system does not recover post the deployment of the fixes, re-assess the incident to determine the root cause
Incident Reporting	• Preparation of postmortem report to capture all the details of the incident

6. Incident Categorisation and Assessment

6.1 The following is the incident categorisation and prioritisation matrix. Examples of incidents provided for each category are non-exhaustive.

Category	Impact	Urgency	Priority
01 – Critical System Failure Complete outage of a primary system supporting the business operation such as the authentication system	**High** Severe financial loss, regulatory breaches, reputational risk	**Immediate**	**P1 – Critical** Target response time: 15 mins
02 – Major Security Breach Breach of customer data or unauthorised access to sensitive applications	**High** Potential legal implications, loss of customer trusts, regulatory penalties	**Immediate**	**P1 – Critical** Target response time: 30 mins
03 – Service Degradation Slowness or partial unavailability of services	**Medium** Disruption to customer service, moderate financial risk	**High**	**P2 – High** Target response time: 1 hour

04 – Minor Technical Issue Issues affecting non-critical system	**Low** Limited operational impact, no direct financial risk	**Medium**	**P3 – Medium** Target response time: 4 hours
05 – Customer Complaint Escalation of customer issues not related to critical system but affecting customer satisfaction	**Low** No direct financial impact, possible reputation risk	**Low**	**P4 – Low** Target response time: 1 business day