Government Data Center

Incident Management Procedure

[Version 1.0]

Revision History

Revision[1] #	Description [2]	Initials [3]	Date [4]
1.0	Initial Incident Management Process draft	NG	12-06-2017

Note

The document will be revised bi-annually.

Throughout this document, following norms will be adopted.

1. Numeric value before decimal represents version of document and after represents number of revision undergone (1.1).

2. Denote changes made in the document (e.g. definition update).

3. Changes made by and approved.

4. Format of the date will be day, month, year.

Overview

The incident management process includes coordination of service recovery, notification, escalation, and event review for all services defined in GDC service catalog. This document is

intended to provide high level overview of the incident management workflow. This document is to be used as reference for all GDC staff and relevant stakeholders to clearly understand the standards and procedures put in place to manage an incident through service restoration and incident review. The document is based on ITIL standards and best practices.

Scope

The incident management process applies to occurrence of all incidents that affect the operation of GDC network and services.

Objective

The primary objective is to to ensure that normal service operation is restored as soon as possible and minimise the adverse impact on business operations, thereby ensuring that best possible levels of service quality and availability are maintained.

Processes

1 Identification

Incidents will be reported in one of the following forms:

1. walk-in,
2. website,
3. phone calls,
4. SMS
5. Emails,
6. Official Social network sites
7. Network Monitoring System
8. BtCIRT
9. Ticketing System(support.govnet.bt)

The service desk then identifies and determines the nature of incident for further assessment.

2 Logging

After identifying and determining the nature of an incident, the Service Desk will log the incident as a ticket. The ticket includes information in the following form:

Name	Contact	Description	Data & Time of Incident

3 Categorisation

It involves assigning category and subcategory to the incident. Service Desk will sort and model incidents based on categories and subcategories. Incidents are categorised as follows:

Categories	Issues
Request	Password Reset, Account Locked
Inquiry/Help	Configuration
Software/Application	MYRBPEMS, RAMIS, eGP
Hardware	CPU, RAM, Storage
Network	IP Address, VPN, DNS
System	Operating System, Migration
Databases	MySQL

4 Prioritisation

An incident's priority will be determined by its impact on users and on the business and its urgency. Urgency is how quickly a resolution is required and impact is the measure of the extent of potential damage the incident may cause.

Based on the impact and urgency, the priority will be given to an incident that will determine how quickly it is scheduled for resolution which is based upon a combination of the incident severity and impact.

Incident Priority	Severity

			3 - Low Issue prevents the user from performing a portion of their duties.	2 - Medium Issue prevents the user from performing critical time sensitive functions	1 - High Service or major portion of a service is unavailable
Impact	3 - Low	One or two personnel/ Degraded Service Levels but still processing within SLA constraints	3 - Low	3 - Low	2 - Medium
	2 - Medium	Multiple personnel in one physical location/ Degraded Service Levels but not processing within SLA constraints or able to perform only minimum level of service It appears cause of incident falls across multiple functional areas	2 - Medium	2 - Medium	1 - High
	1 - High	All users of a specific service/ Personnel from multiple agencies are affected/ Public facing service is unavailable	1 - High	1 - High	1 - High

5 Incident Response

After identifying, categorizing, prioritizing, and logging the incident, the service desk will handle and resolve the incident. Incident resolution will involve five steps as follows:

5.1 Initial diagnosis

Users will describe problem and respond to all basic troubleshooting questions.

5.2 Incident escalation

The Service Desk will monitor all incidents, and escalate them based on the following metrics:

Priority	Time Limit before Escalation
3 - Low	3 business days
2 - Medium	4 hours
1 - High	Immediate

When the Service Desk receives notification of an incident, initial identification and diagnosis will be carried out to classify the incident according to service category and prioritization. In case the incident is a known problem with a known solution, the Service Desk will attempt a resolution. In case it is not a known problem or if the attempted solution fails, responsibility for an incident will be delegated to an appropriate expert group.

5.3 Investigation and diagnosis

These processes take place during troubleshooting when the initial incident hypothesis is confirmed as being correct. Once the incident is diagnosed, a solution should be applied, such as changing software settings, applying a software patch, or ordering new hardware.

5.4 Resolution and recovery

This is when the service desk confirms that the user's service has been restored to the required SLA level.

Incident support for existing services is provided 8 hours per day[9AM-5PM] during weekdays and on-call support during weekends and public holidays. Following are the current targets for response and resolution for incidents based upon priority.

Priority	Target	
	Response Time	Resolution Time
3 - Low	90% - 24 hours	90% - 7 days
2 - Medium	90% - 2 hours	90% - 4 hours
1 - High	95% - 15 minutes	90% - 2 hours

5.6 Incident closure

The incident process ends after the incident is closed. In case an incident is caused due to force majeure incidences, other appropriate measures will be adopted with prior approval from the concerned authority.