SMG 3210.13

FDA STAFF MANUAL GUIDES, VOLUME III - GENERAL ADMINISTRATION

INFORMATION RESOURCES MANAGEMENT

INFORMATION TECHNOLOGY MANAGEMENT

POST INCIDENT RESPONSE POLICY

Effective Date: 11/29/2017

1. PURPOSE

The purpose of the Food and Drug Administration's (FDA) Post Incident Response Policy is to outline requirements to identify, diagnose, and document root causes of associated incidents and/or disruption of operational services. An incident is defined as an unplanned interruption or reduction in quality of an IT service.

2. BACKGROUND

Problem Management includes the activities required to diagnose the root cause of incidents identified through the Incident Management (IM) process, and to determine the resolution to those problems. It includes activities for ensuring that the resolution is implemented through the appropriate control procedures. The IM process also maintains information about problems, the appropriate workarounds and resolutions so that the Office of Information Management and Technology (OIMT) can reduce the number and impact of incidents over time.

Although IM and Problem Management are separate processes, they are closely related and will typically use the same tools, and may use similar categorization, impact and priority criteria.

While problem management does strive to identify the root cause(s), it also seeks to identify contributing causes that elongate outages, opportunities to prevent outages or reduce their impact, and ensures that these tasks are actively tracked to resolution. Ultimately, the goal is to eliminate high-priority incidents and sharply reduce recurring incidents.

3. POLICY

Under the authority of the OIMT government representatives, Systems Management Center (SMC); Information Technology Call Center (ITCC); and appropriate support stakeholders i.e., Systems/Application Owners/Restoration Teams, shall ensure the timely identification, diagnosis, and documentation of root causes of associated incidents and/or disruption of operational services. Priority 1 and Priority 2 Post Incident Reports shall identify root causes within 24 hours with a complete Root Cause Analysis (RCA) completed within 72 hours of incident resolution.

Specifically, the following information shall be collected and documented in the Post Incident Report to support this Post Incident Policy:

- Problem Definition
- Description of the problem (identity, location, duration and impact)
- Identified scope of impact to FDA business area(s).
- Corrective steps taken to resolve the incident
- Improvements needed to prevent the recurrence of similar incidents.
- Description of issue and corrective steps added to Knowledge Base.

RCA should be used for identifying the root causes of faults or problems; factors that caused the incident, increased the priority of the incident, delayed resolution of the incident, or prevented detection of the incident prior to impact.

The Post Incident Report including RCA shall be delivered, reviewed and signed by appropriate technical monitors and IT managers and posted in the Post Incident Report/Root Cause Analysis area within 72 hours to allow the CIO, center ADCIOs, and Deputy CIOs to review the resolution of the incident.

Additionally, a weekly summary report that details all Priority 1 and 2 incidents and/or outages from the previous week shall be produced. The summary report shall be provided to the Deputy CIOs, center ADCIOs, and all OIMT Division Directors.

Weekly summary reports shall be in a standard format that includes but is not limited to:

- Date/Time and Length of Outage
- Network, Systems, and/or Applications affected

- Scope of Impact to FDA customers and systems
- Users/Customers affected
- Reason for Outage
- Root Cause and/or Problem
- Remediation Actions

4. RESPONSIBILITIES

A. FDA Chief Information Officer (CIO).

The CIO provides leadership and direction regarding all aspects of the Agency's information technology (IT) programs and initiatives including operations, records management, systems management, information security, strategic portfolio, and executive coordination and communication activities.

B. Deputy CIO, Office of Technology and Delivery (OTD).

The Deputy CIO, OTD is responsible for the execution and implementation of infrastructure operations and application services policy and procedures throughout the FDA enterprise.

C. Deputy CIO, Office of Business and Customer Assurance (OBCA).

The Deputy CIO, OBCA is responsible for all business process systems under the management of OIMT, including training, user guides, help desk support, and troubleshooting. The OBCA develops, refines, executes, and monitors compliance with customer service level agreements.

D. FDA Chief Information Security Officer (CISO).

The CISO serves as the Agency focal point to direct and oversee the IT Security Program within the Agency and oversight of the Systems Management Center.

E. Information Technology Call Center (ITCC) Representative.

The ITCC Representative coordinates, analyzes, researches, and diagnoses Tier 1 solutions for desktop communication and connectivity issues related to the intranet, Wide Area Networks (WANs), Local Area Networks (LANs), Virtual Private Networks (VPNs), remote access and other network, systems, and applications technologies. The representative interfaces with FDA customers in the identification of service disruptions, outages, and events, and documents the following information to support the resolutions of incidents:

- Name of system, function, or application
- Detailed description of the Incident (Number of users affected/Business Impact)
- Customer name, contact phone number and location

F. Systems Management Center (SMC)

The SMC Watch Officers direct the around the clock operations supporting cybersecurity operations, network and application monitoring. They direct all SMC monitoring, response, and notification actions during an assigned shift in accordance with established processes/procedures. They direct the triage of network and application outages, while facilitating collaboration across multiple groups to respond to and remediate the outage. They coordinate alerts and updates to all stakeholders and provide response actions as outlined here:

- Coordinate service disruptions and outages with the Restoration Teams.
- Direct and manage the technical solutions bridge to resolution
- Ensure timely status updates to ITCC, Senior Leadership Team, and Division Directors.
- Work to reduce impact as rapidly as possible.
- Identify technical/operation solutions and/or work-arounds.
- Document all coordination and trouble-shooting activities.

G. Systems/Application Owners/Restoration Teams.

They coordinate and assist in the restoration of disrupted services, outages, and incident/events related to affected networks, infrastructure, systems, applications and databases. They provide timely updates to the SMC Watch Officer and ITCC Representatives and assist with the creation of Incident tickets, RCAs, Post Incident Reports, etc..

5. PROCEDURES

Refer to the SMC Concept of Operations, Division of Infrastructure Operations (DIO) Data Center Application and Infrastructure Incident Management Procedure, and the Division of Business Partnership and Support Customer Alert Notification Standard Operating Procedures for detailed instruction and guidance.

6. REFERENCES

- Systems Management Center Concept of Operations (CONOPS)
- PCD-ESM-0050 Data Center Application and Infrastructure Incident Management Procedure 5/17/2015

- Customer Alert Notification Standard Operating Procedures
- Clinger-Cohen Act Public Law 104-106 of 1996
- Federal Information Security Management Act (FISMA) of 2002
- Office of Management and Budget (OMB) Circular A-130
- HHS CIO Policy for Information Systems Security and Privacy
- FDA Incident and Response Procedure Guide of 2016

7. EFFECTIVE DATE

The effective date of this guide is November 29, 2017.

8. Document History – SMG 3210.13, Post Incident Response Policy

STATUS (I, R, C)	DATE APPROVED	LOCATION OF CHANGE HISTORY	CONTACT	APPROVING OFFICIAL
Initial	11/28/2017	N/a	Deputy CIO, Office of Technology and Delivery (OTD)	Todd Simpson, FDA Chief Information Officer

Back to General Administration, Volume III (2000-3999)