**SMG 3210.12**

# FDA Staff Manual Guides, Volume III - General Administration

## Information Resources Management

## Information Technology Management

## Service Disruption Outage Response Policy

Effective Date: 12/04/2017
Changed: 11/01/2021

## 1. Purpose.

The purpose of the Food and Drug Administration’s (FDA) Service Disruption Outage Response policy is to outline requirements to ensure timely response and restoration of services and to minimize adverse impact to mission and business operations.

## 2. Background.

Disruption to operational services can be planned or unplanned. This policy addresses unplanned outages. The Incident Management process will be executed upon the identification and/or notification of an unplanned outage or event. Incident Management is the process by which unplanned outages or events are managed, with the objective to restore normal service operation and to minimize the adverse impact on mission and business operations. An Incident may be triggered by any event, not part of a standard service operation, which causes, or may cause an interruption or reduction in quality of service and customer productivity

The Systems Management Center (SMC) is a central command and control center, available around the clock, for the monitoring, triaging, troubleshooting, and the escalation of all detected, reported or potential security incidents, performance issues, enterprise services, applications services and infrastructure operations. The SMC operational capabilities are established to enhance the Office of Information Management and

Technology's ability to conduct highly effective incident response, improve situational awareness, and strengthen our overall operational posture.

While the SMC is aligned under the FDA Chief Information Security Officer (CISO), Office of Digital Transformation (ODT), Office of Information Security; the operational, technical, and coordination function is a shared responsibility of the Division of Infrastructure Operations, Division of Application Services, and Division of Business and Partnership Support.

The Information Technology Call Center (ITCC) plays an integral role and is the primary interface for FDA Centers, Offices, and employees for outage reporting, notification, information, and response.

## 3. Policy.

This Service Disruption Outage Response policy outlines specific response times to minimize adverse impact and disruption to FDA mission and business operations.

When a potential incident has been reported to the SMC, through any of these mechanisms, the SMC will open an Incident ticket, recording the affected user(s), affected Configuration Items (CI's), date and time, and any other information provided by the automated tools or user/administrator reports. The SMC will then attempt to confirm the incident, through troubleshooting and contact with the official Point of Contact for the affected CI's.

Confirming an Incident involves the determination that an actual fault has occurred (not a false alarm), ensuring that the outage is persistent and not transient, and assessing the impact.

Once an incident is confirmed, SMC will assign the associated Incident ticket(s) to the appropriate support stakeholders i.e., Systems/Application Owners/Restoration Team(s). The responsible team must then respond to the ticket within the time frames described below, depending on Incident Priority:

| **Outage Priority Levels** |
|---|
| Priority Level 1 – Emergency/Urgent Critical Business Impact<br>The incident has caused a complete and immediate mission disruption affecting a critical function or critical infrastructure component in a Production application or system, such that a primary business process or a large group of users such as an entire department, floor, branch, line of business, or external customer experience a complete degradation/disruption of service. Examples: Major application incident effecting enterprise services (e.g. VPN remote access). Severe disruption during critical periods WAN or LAN outage, or security incidents (e.g., denial of service).<br>NOTE: All Development, Test and Pre-Production Systems are Priority Level 3.<br>Priority Level 1 Time to Notify Senior Agency Leadership<br>< 15 Minutes |
| Priority Level 2 – High Major Business Impact<br>A business process is affected in such a way that business functions are severely degraded, or a critical function is operating at a significantly reduced capacity or functionality in a Production application or system. Examples: System or application is performing slowly or fault tolerance is impacted. Typically, a work around is available and the workload is manageable.<br>Priority Level 2 Time to Notify Senior Agency Leadership<br>< 30 Minutes during Business Hours (Monday-Friday 6AM-9PM)<br>< 60 Minutes – Non-Business Hours and Holidays |
| Priority Level 3 – Medium Business Impact<br>A business process is affected in such a way that some functions are unavailable to end users or a system and/or service is degraded. Examples: End-User Device incident (e.g., hardware, software). Development, Test and Pre-Production systems fall under Priority Level 3 unless significant circumstances exist.<br>Priority Level 3 - Senior Agency Leadership is not normally notified outside of standard incident reporting unless significant circumstances exist. |

Priority Level 4 – Low to minimal Business Impact

An incident that has minimal impact on normal business processes and can be handled on a scheduled basis as there is minimal negative impact on a user's ability to perform their normal daily work. Example: Service Requests (e.g., system enhancement, changes installations), Preventative Maintenance).

Priority Level 4 – Senior Agency Leadership is not normally notified outside of standard incident reporting.

Throughout the lifecycle of the incident, the incident ticket will be updated along with actions taken, and ongoing developments.

The SMC is then responsible for communicating the Incident to Management, and the escalation group(s) of the impacted user groups, e.g., centers.

SMC will produce and disseminate initial Service Outage Notifications within the prescribed timeframes for a confirmed Incident. If positive contact cannot be made within the timeframe window, but the indication of an Incident persists, then the SMC will produce and disseminate an initial Service Outage Notification appropriately.

Once a Service Outage Notification has been sent, updates must be sent every 30 minutes thereafter conveying any actions taken and/or changes in status for Priority Level 1 and 2 Incidents. For ongoing incidents, these may be suspended after the first update if no change in status has occurred.

Once a fault has been repaired, the SMC or the responsible Tier III team must confirm that the impacted users can access the affected CI. The fix action is recorded in the Incident ticket, and communicated to the SMC. The SMC summarizes the fix action into a Service Outage Resolution, sent to Management and the escalation group(s) of the impacted users.

After the closure of the Incident, a Root Cause Analysis process will be invoked to analyze the response on all Priority Level One tickets/incidents.

## 4. Responsibilities.

### A. FDA Chief Information Officer (CIO).

The FDA 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. 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.

**C. Information Technology Call Center (ITCC) Representative.**

ITCC Representatives coordinate, analyze, research, and diagnose Tier1 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. Interface with FDA customers in the identification of service disruptions, outages, and events by distributing notifications Agency wide on ongoing issues. Documents the following information to support the resolutions of incidents:

1. Name of system, function, or application

2. Detailed description of the Incident (Number of users affected/Business Impact)

3. Customer name, contact phone number and location

**D. SMC Watch Officer.**

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

1. Coordinate service disruptions and outages with the Restoration Teams.

2. Ensure timely status updates to ITCC, Senior Leadership Team, and Division Directors.

3. Work to reduce impact as rapidly as possible.

4. Identify technical/operation solutions and/or work-around.

5. Document all coordination and trouble-shooting activities

### E. Systems/Application Owners/Restoration Teams.

Systems/Application Owners/Restoration Teams coordinate and assist in the restoration of service disruptions, outages, and incident/events, related affected networks, infrastructure, systems, applications and databases. They provide timely communications with SMC Watch Officer and ITCC Representatives.

## 5. Procedures.

Refer to the SMC Concept of Operations, Division of Infrastructure Operations Incident/Problem Management procedures, and the Division of Business Partnership and Support Customer Alert Notification Standard Operating Procedures for detailed instruction and guidance.

## 6. References

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

## 7. Effective Date.

The effective date of this guide is December 4, 2017.

## 8. Document History - SMG 3210.12, Service Disruption Outage Response Policy

| Status (I, R, C) | Date Approved | Location of Change History | Contact | Approving Official |
|---|---|---|---|---|
| Initial | 09/14/2017 | N/a | Office of Technology and Delivery (OTD) | Todd Simpson, FDA Chief Information Officer |
| Revision | 12/03/2017 | N/a | Office of Technology and Delivery (OTD) | Todd Simpson, FDA Chief Information Officer |
| Change | 10/27/2021 | Removed two roles from Section 4, Responsibilities | Office of Technology and Delivery (OTD) | FDA Chief Information Officer |