



**Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)**

Major Incident and Disaster Management Procedure

I. Statement

This Procedure establishes OIT's command, control, and communication protocol for managing Major Incidents and Disasters.

II. Purpose

Working through a pre-defined Procedure, Agencies and OIT will collectively ensure the best possible response to Major Incidents and Disasters.

III. Applicability

This policy applies to:

1. The Executive Branch and *Semi-autonomous State Agencies*, irrespective of where their applications are hosted
2. Applications from other State government branches that are hosted on devices operated by the OIT, or those that traverse the State's wide area network.

IV. Responsibilities

- A. Chief Information Officer (CIO): Declares a Disaster and communicates with Commissioners.
- B. Chief Technology Officer (CTO): Declares a Major Incident, and owns, executes, and enforces this Procedure.
- C. Manager, Customer Support (Help Desk): Identifies potential Major Incidents (unless already identified by an Operational Manager), notifies other appropriate parties, and updates the OIT Customer Support Status Page.
- D. Operational Managers: Identify potential Major Incidents (unless already identified by the Manager, Customer Support (Help Desk), notifies other appropriate parties, and participates in the remediation.
- E. Duty Manager: Facilitates the remediation.
- F. Incident Commander: Owns, manages, and leads the response and remediation to Major Incidents and Disasters.

Major Incident Management Procedure

- G. Technology Business Consultants: Own all communication and liaison to the affected Agencies.
- H. Incident Communicator: In order to concentrate more exclusively on the response and remediation, the Incident Commander may optionally delegate the communication and coordination to a dedicated Incident Communicator.
- I. Incident Command Team: The Incident Commander must pull together the Incident Command Team ASAP. In practical terms, the initial contacts are likely to occur via phone and e-mail. While a virtual team is possible, it is preferable to manage the incident from an OIT site. A conference room or an office may be commandeered as the ad-hoc Incident Command Center.
- J. Enterprise Security Officer: Advises the Incident Commander in case of security breaches.
- K. Key Agency Personnel: Must be kept informed every step of the way by the Technology Business Consultants, and in some cases, be subsumed within the Incident Command Team.
- L. Vendors: At the discretion of the Incident Command Team Lead, key vendor(s) may be subsumed within the Incident Command Team.
- M. Root Cause Resolution Team: An optional investigative team created post-remediation to investigate root cause(s).

V. Directives

A. Awareness & Initiation

1. Whenever the Manager, Customer Support (Help Desk) or an Operational Manager becomes aware of a *potential* Major Incident or Disaster, based on either calls or internal monitoring, they immediately notify the other party, the Duty Manager, and the Incident Commander.
2. The Incident Commander collects as much detail as possible from the Manager, Customer Support (Help Desk) and the Operational Manager, and calls the CTO and/or the CIO to resolve two basic questions (see below).
3. The CTO makes the judgment call on whether this Incident qualifies as a Major Incident. The CIO makes the judgment call on whether this Incident qualifies as a Disaster. Either way, at the end of this step, the Incident Commander will know the following two things: (1) The proper classification of this Incident, i.e., whether this Incident actually rises to the level of a Major Incident or Disaster, and (2) Quantitative metric(s) of what constitutes remediation of this Incident.

B. Response

Major Incident Management Procedure

1. The Incident Commander gathers the Incident Command Team. In practical terms, the initial contacts are likely to occur via phone and e-mail. A call-in number will be provided by the Incident Commander to the Incident Command Team members if used.
2. The Incident Commander consults with the just-formed Incident Command Team.
3. The Incident Commander optionally identifies an Incident Communicator.
4. Upon instructions from the Incident Commander (or the Incident Communicator), the Manager, Customer Support (Help Desk), updates the OIT Customer Support Status Page. To the extent known at the time, the update covers:
 - (1) The nature of the Incident in plain language,
 - (2) The projected impact on Agency operations and/or citizens,
 - (3) Quantitative metric(s) of what constitutes remediation,
 - (4) The remediation steps being undertaken,
 - (5) Estimated time for remediation, and
 - (6) Estimated next update time.
5. The CIO/CTO/Incident Commander, at their discretion, provide initial and update notifications to the DAFS Commissioner, the DAFS Communications Director, and affected Agency Commissioners.
6. The Incident Commander (or the Incident Communicator) notifies the affected Technology Business Consultants.
7. The Incident Commander activates the Incident Command Center at Room 412 (Operations/Training Room), 4th floor, 51 Commerce Center Drive, Augusta, to lead/facilitate the remediation.
8. At their discretion, the Incident Commander reaches out to any vendor/supplier as well as Key Agency Personnel for inclusion into the Incident Command Team.
9. The Incident Commander manages the Incident Command Team and leads/facilitates the remediation. In doing so, the Incident Commander initiates any and all necessary steps, including reaching out to any and all OIT resources (while briefing their command chains), initiating conference calls with vendors, suppliers, partners, Key Agency Personnel, et al., as well as any other necessary remediation steps.
10. The Incident Commander (or the Incident Communicator) notifies other OIT personnel as necessary, including, but not limited to, the OIT Extended Managers and affected OIT staff.
11. The Technology Business Consultants ensure that the affected Agencies are adequately briefed.
12. The Incident Commander (or the Incident Communicator) ensures that the OIT Customer Support Status Page is updated no later than the estimated update time posted most recently, until remediation. To the extent known, each update must cover the six items identified above.

Major Incident Management Procedure

13. In case of a security breach, the Incident Commander will reach out to the Enterprise Security Officer for further advice. State Law¹ mandates notifications under certain kinds of security breaches.

C. Diagnosis & Remediation:

1. Affected Operational Managers and their teams (in all likelihood, already part of the Incident Command Team) diagnose the cause, and estimate time to remediation.
2. At all times, the Operational Managers ensure without fail that the Incident Commander is fully briefed.
3. The Incident Commander creates a Major Incident ticket in the Footprints Major Incident project.
4. Operational Managers & their teams perform necessary remediation. All changes must follow pre-established emergency change control procedures.
5. The Incident Commander determines if and when the remediation quantitative metric(s), decided previously, have been met.
6. Restoration Priority Order (Subject to approval by the Governor's Office):
 - (1) Core Information Infrastructure, such as network, email, etc.
 - (2) Citizen Health & Safety
 - (3) Revenue
 - (4) Citizen Financial Services
 - (5) Regulation
 - (6) Provider/Vendor Financial Services
 - (7) All Other Services

D. Post-Remediation:

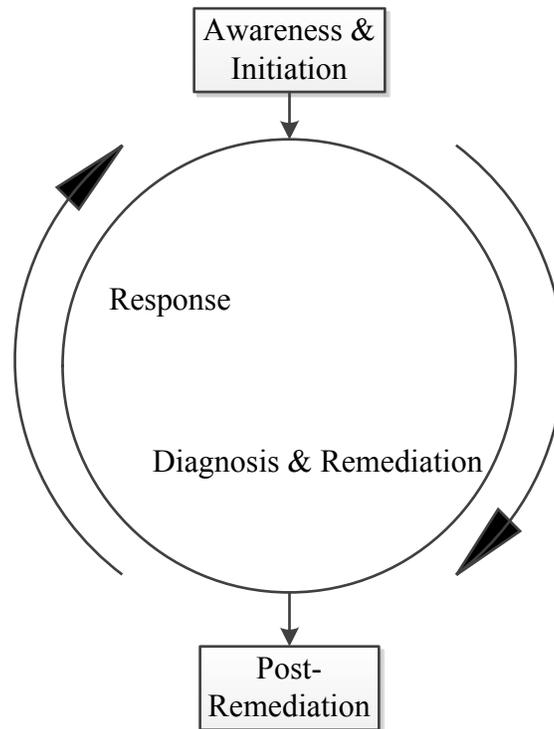
1. Operational Managers and their teams document the Footprints Major Incident ticket.
2. The Incident Commander ensures that any follow-up activities are logged as tickets in the Footprints Major Incident project.
3. In some cases, the Operational Managers and their staffs will be able to remediate with a workaround, even without successfully identifying the root cause. In such cases, the Incident Commander may downstream create a Root-Cause Resolution Team to investigate root cause(s) and recommend permanent solutions.
4. At the conclusion of an incident, the Root-Cause Resolution Team will create a preliminary report for distribution to the impacted customers within two business days (48 hours). This preliminary report will be followed by additional documentation,

¹ Notice of Risk to Personal Data, Title 10, Chapter 210-B,
<http://www.mainelegislature.org/legis/statutes/10/title10sec1347.html>

Major Incident Management Procedure

according to the OIT Major Incident Report in the Appendix, for distribution to all concerned parties, within five business days of the incident. Both reports must be reviewed by the CIO and/or the CTO prior to distribution. Once approved, they may be distributed and attached to the Footprints Major Incident ticket.

E. The following diagram represents the flow-sequence among the four steps.



VI. Definitions

A. Disaster: An Incident that the Chief Information Officer judges to have a *catastrophic* impact on governmental information operations. Examples include:

- Fire in one of the OIT data centers, disabling the majority of information operations.
- Cyber-attack that shuts down the entire State network.

B. Incident: An Incident is any unplanned event that *potentially* disrupts governmental information operations. However, this Procedure does *not* cover Incidents that do not actually rise to the level of either Major Incidents or Disasters.

C. Major Incident: An Incident that the Chief Technology Officer judges to have a *significant* impact on governmental information operations. Examples include:

- Network, email, or other app outage, for two hours or longer, significantly affecting governmental productivity and/or public service.

Major Incident Management Procedure

- Security breach, significantly compromising either the credibility or operational capability of the government.

D. Operational Manager: A line manager with whom a potential Major Incident is first raised by their staff.

E. Semi-autonomous State Agency: An agency created by an act of the Legislature that is not part of the Executive Branch. This does not include the Legislature, the Judiciary, the Office of the Attorney General, the Office of the Secretary of State, the Office of the State Treasurer, and the Audit Department.

VII. References

VIII. Document Information

Adoption Date: February 26, 2014

Effective Date: February 26, 2014

Review Date: February 26, 2016

Point of Contact: B. Victor Chakravarty, Enterprise Architect, Office of Information Technology, State House Station #145, Augusta, ME 04333, (207) 624-9840.

Approved By: James Smith, Chief Information Officer, State House Station #145, Augusta, ME 04333, (207) 624-9424.

Position Title(s) or Agency Responsible for Enforcement: Greg McNeal, Chief Technology Officer, Office of Information Technology, State House Station #145, Augusta, ME 04333, (207) 624-9424. 624-9471

Legal Citation: 5 M.R.S.A. Chapter 163 Section 1973 paragraphs (1)B and (1)D, which read in part, “The Chief Information Officer shall: “Set policies and standards for the implementation and use of information and telecommunications technologies...” and “Identify and implement information technology best business practices and project management.”

Waiver Process: See the [Waiver Policy](#)².

IX. Appendix

OIT Major Incident Report

FootPrints Major Incident Ticket ID#

Summary

A paragraph or two of short description, each paragraph beginning with date and time. E.g.: 11/05/2011 03:00h, noticed that D disk on web server Boo came to 98% full

² <http://maine.gov/oit/policies/waiver.htm>

Major Incident Management Procedure

Impact

I. End User Impact:

Short description of what the impact was on users

II. Impacted Services:

Services impacted	Minutes of full service downtime	Minutes of severely reduced QOS	Total minutes	SLA impact [%]	Time From-To	No. of users impacted by downtime
Service1						
Service 2						

Incident Start Date and Time

dd.mm.yyyy. hh:mm

Service Restoration Date and Time

dd.mm.yyyy. hh:mm

Incident Root Cause

Short description of the root cause, few paragraphs max.

Incident Resolution Course

Incident Timeline

Resolution type

Select one:

- Fully resolved. Root cause identified. Unlikely to recur
- Resolved by workaround. Root cause not determined. Known issue. No further action
- Resolved by workaround. Root cause not determined. May recur.

Lessons Learned & Planned Actions

1. What are the lessons learned?
2. Institute products and/or processes to prevent recurrence.
3. Each Footprints ticket has space for several follow-up assignments and date ranges. If there exist complex or multiple follow-up assignments, sub-task tickets are created from the Major Incident ticket.

Footprints Incident Project

Footprints ticket #		
Follow up task	Assigned to:	Due Date: