



OVERVIEW OF MAJOR INCIDENT PROCESS FOR DCSS

DIVISION OF INFORMATION TECHNOLOGY
JOYCE LANDRETH, JLANDRET@VT.EDU
LUCAS SULLIVAN, LUCAS.SULLIVAN@VT.EDU
TERESA SNAVELY, TSNAVELY@VT.EDU



OBJECTIVES



1

2

3

4

5

What is a Major Incident?

Summary of the goals and steps in the Major Incident process.

Identifying an incident as a potential major incident.

Responsibilities and roles for the Major Incident Process/Communication Paths.

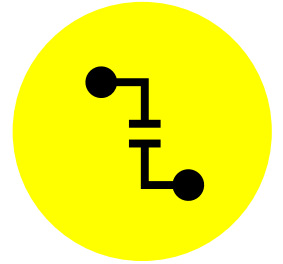
Tabletop exercises and continuous improvement.



What is a Major Incident?



CORE SERVICE



INCIDENT



MAJOR INCIDENT



CRITICAL
SERVICE



PROBLEM





MAJOR INCIDENT PROCESS

Goals of the process

- Restore normal service operation
- Engage persons and teams for fast resolution
- Keep stakeholders situationally informed
- Support continued improvement through after-action reviews

Main steps of the process

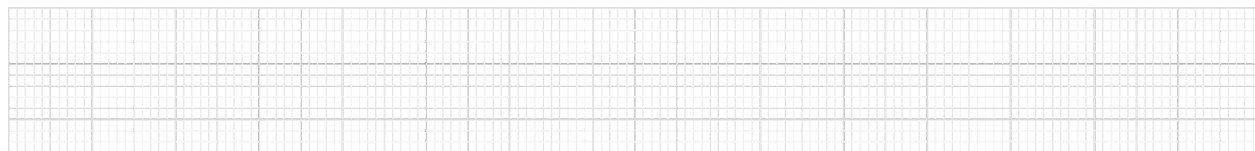
1. Identification
2. Mitigation and communication
3. Resolution
4. After Action Review (AAR)



Identification Triggers for Major Incident Proposal

- Core or critical Service
- Impact and urgency is high priority or critical
- Cause of many incidents or potential cause to many incidents
- Indicators of an outage or degradation
- Time critical business processes are disrupted

Prioritization Matrix		Urgency			
		Critical	High	Normal	Low
Impact	University	P1	P1	P2	P4
	Multiple users/building(s)	P1	P2	P2	P4
	Single User	P2	P2	P3	P4





Roles and Responsibilities

All Roles

4Help

Frontline IT support

Identify

Identify a major incident

Propose

Propose a major incident

Associate

Associate an incident with a major incident

Awareness

Stay aware of the status of the major incident



Roles and Responsibilities

Service Owner
Technical Lead
Assignment/Support
Group

Notifications

Sign up for SMS notifications for Major Incidents

Coordinate

Service Owner gives input to communications and coordinates efforts of technical lead

Troubleshoot

Technical lead directs troubleshooting of the team

Communicate

Interact in the war room and update changes in the major incident channel

After-action Review

Participate in and update the after-action review



Roles and Responsibilities

Major Incident Manager

Notification

Sign up for SMS notification for Major Incidents

Coordinate

Major Incident Manager Checklist and manage the Major Incident

Promote

Monitor major incident candidate. Investigate, and promote

Communicate

Set up war room and major incident channel

Resolve

Resolve the Major Incident



COMMUNICATION

Notification emails from ServiceNow using templates

Provides standard information

Populates info from the MI record

Allows for edits

MI Manager responsible

Backup communication



COMMUNICATION

Communication will be handled by the MI manager from the Major Incident using Workbench.

Communication Tasks

All▼Add

Technical Communications 0 / 3 Tasks completed

Add Task⋮^

➔

Initial Technical Communication

Due in 00:11:54

Send⋮

Channels:

E-mail

Status:

Not sent

Order:

100

Assigned to:

David Duckett

☐

Technical Status Update

Send⋮

Channels:

E-mail

Status:

Not sent

Order:

200

Assigned to:

David Duckett

☐

Technical Resolution Communication

Send⋮

Channels:

E-mail

Status:

Not sent

Order:

300

Assigned to:

David Duckett

Internal Stakeholder Communications 0 / 3 Tasks completed

Add Task⋮^

➔

Initial Stakeholder Communication

Due in 00:11:45

Send⋮

Channels:

E-mail

Status:

Not sent

Order:

100

Assigned to:

David Duckett

☐

Stakeholder Status Update

Send⋮

Channels:

E-mail

Status:

Not sent

Order:

200

Assigned to:

David Duckett

☐

Stakeholder Resolution Communication

Send⋮

Channels:

E-mail

Status:

Not sent

Order:

300

Assigned to:

David Duckett

MAJOR INCIDENT OVERVIEW

major

Incident

▼ Major Incidents

Overview

Create Major Incident Candidate

Candidates

Open

All

Major Incident Overview

OverviewMajor Incident CandidatesActive Major IncidentsResolved Major Incidents

Major Incidents Nearing Breach0

Major Incidents Overdue0

Unassigned Major Incidents0

Open Major Incidents12

Major Incidents Opened Today0

Major Incidents Resolved Today0

Open Major Incidents - Grouped

Open Major Incidents Older Than 7 Days - Grouped

Major Incidents by Priority and State

Major Incidents by Priority and State older than 7 Da

2 - High

1 - Critical

3 - Normal

0123456

Major Incide...

Group byPriorityStacked by-- None --

2 - High

1 - Critical

3 - Normal

0123456

Major Incide...

Group byPriorityStacked by-- None --

1 - Critical

2 - High

3 - Normal

ActiveAwaiting ProblemAwaiting User InfoResolved

1 - Critical

2 - High

3 - Normal

ActiveAwaiting ProblemAwaiting User InfoResolved

Continuous Improvement:

Tabletop Exercises

