Policy Title Major Incident (Priority 1)
Department Information Services
Chapter 5
Section 9
Policy 1
Effective Date Thursday, April 1, 2021

POLICY STATEMENT

The purpose of this policy is to provide clear guidance regarding "Major Incident (Priority 1)" handling from the point of detection and logging through resolution so that "normal" service operation is restored as quickly as possible.

This will help enable IS to:

- Minimize the adverse impact of major Incidents on business operations.
- Ensure that the best possible levels of service quality are maintained.
- Enhance the level of Customer satisfaction with the Incident resolution process.

Consistent execution of the tenets contained within this policy will also result in:

- A higher level of efficiency within IS workgroups involved in the Priority 1 Incident resolution process.

APPLICABILITY

All IS personnel who execute and/or manage the major priority 1 incident management process are to align with this policy.

GENERAL INFORMATION

Policies

- The Service Desk must be notified of all priority 1 incidents.
- All priority incidents will be logged in Cherwell. The parent ticket will be owned by the incident manager. The child tickets will be assigned to the functional teams.
- Service support hours for priority 1 incidents are 7x24x365.
- Major, priority 1 incidents shall be resolved in alignment with described roles, responsibilities, processes, and procedures.
- The response time objective for the functional assignee group is 15 minutes. Response time is defined as when the assignee group acknowledges the ticket in the system.
- The resolution time service level objective for priority 1 incidents is 4 hours from the time the incident was logged.
- The Incident Manager shall facilitate resolution of priority 1 incidents utilizing a "swarming" (team) approach.
- The Incident Manager shall be responsible for internal communication to relevant parties as outlined in this policy and related procedures. (See Communication and Notification table below.)
- Communications shall be responsible for external communication to relevant parties if warranted.
- Emergency Management shall be responsible for emergency communications through Everbridge to relevant parties if warranted.
- All priority 1 incidents for which a root cause and/or permanent, cost-effective fix is unknown shall result in a Problem record that will be addressed as the highest priority.
- The post-incident review (PIR) shall be conducted within three (3) business days of incident close; the PIR report shall be distributed with two (2) business days after the review.
- All priority 1 incidents shall follow the prescribed process unless an exception is approved by the Incident Management Practice Owner.
- If the P1 incident includes data breaches, refer and adhere to the Security Incident Management Policy and Standard.

Process

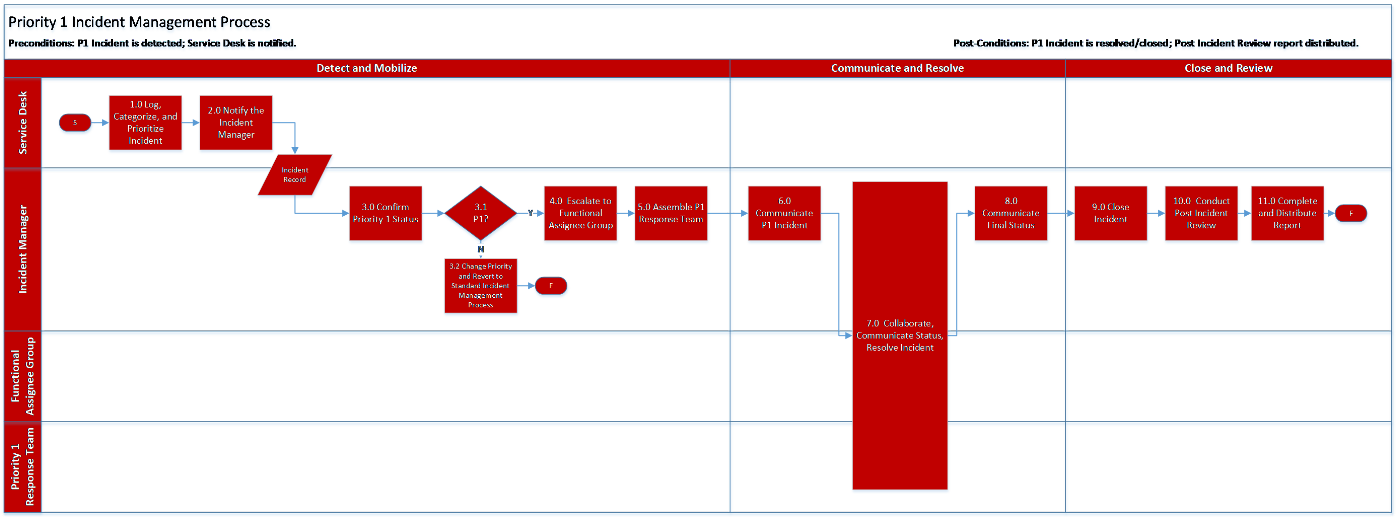
"Major" Priority 1 Incident Process

Communication/Notification

Communication is critical due to the overall impacts of a priority 1 incident.

The Incident Manager will communicate with internal, relevant stakeholders in alignment with these minimal standards. Communications is responsible for determining the appropriate strategy for and executing external communications.

Step #	Notification/Communication	Media*/Timescale
1	Incident submission	Initial IT Service Alert (ITSA) within 30 minutes of P1 confirmation.


Priority 1 Incident Management Process
Preconditions: P1 Incident is detected; Service Desk is notified.
Post-Conditions: P1 Incident is resolved/closed; Post Incident Review report distributed.
Detect and Mobilize
Communicate and Resolve
Close and Review
Service Desk
Incident Manager
Functional Assignee Group
Priority 1 Response Team
S
1.0 Log, Categorize, and Prioritize Incident
2.0 Notify the Incident Manager
Incident Record
3.0 Confirm Priority 1 Status
3.1 P1?
Y
N
3.2 Change Priority and Revert to Standard Incident Management Process
F
4.0 Escalate to Functional Assignee Group
5.0 Assemble P1 Response Team
6.0 Communicate P1 Incident
7.0 Collaborate, Communicate Status, Resolve Incident
8.0 Communicate Final Status
9.0 Close Incident
10.0 Conduct Post Incident Review
11.0 Complete and Distribute Report
F

*Email is the preferred medium; phone updates will be utilized as deemed appropriate.

Metrics/performance measures

Priority 1 incident management performance will be measured through the following key performance indicators:

- Response time: The functional team has 15 minutes to response to escalated ticket.
- Resolution time: 4 hours from the time the incident is logged.
- Communication targets: See table above.
- Post-incident review (PIR): Three business days from resolution.
- Post-incident review (PIR) report: Distributed withing two business days after the review.
- Exceptions to this policy will be measured and reported.

Exceptions

It is recognized that there may be situations in which it is in the best interest of impacted stakeholders to deviate from the expectations outlined in this policy. Requests for exceptions to this Policy must be approved before implemented by the Incident Practice Owner. The exception will be recorded and included in operational reports by the Incident Management Practice Manager.

Audit

The Incident Management Practice Owner shall audit a sample of Incident Management-related documentation to ensure compliance to the Incident Management Policy, Process, and Procedures (minimally once a year).

AUTHORITY

This policy and the procedures herein were prepared under the authority of the County Manager, as delegated to the Ramsey County Chief Information Officer.

DEFINITIONS

An “Incident” is defined as “an unplanned interruption to a service or reduction in the quality of that service” (ITIL® v4). A “major” or “priority 1” incident is defined in the “applicability” section of this policy document.

This policy pertains to “major” or “priority 1” incidents which are defined as technology outages which are Department/County-wide and thus have a massive impact, resulting in the inability to perform a critical job function. “Critical job function” refers to those business processes that are deemed vital to serve Ramsey County residents and for which there is no redundancy or acceptable manual workaround. They are essential for County service delivery to residents and/or customers. Without these systems:

- Business operations stop, or
- Life, safety or security are threatened, or
- Violation of legal rights, or
- Systems environment will be crippled.

Note: Business cycles may dictate when certain systems are deemed critical as "priority" is a result of "impact" and "urgency."

Examples of priority 1 incidents include:

- Enterprise e-mail or enterprise messaging outage or impaired service
- County portal services down or impaired
- VOIP phone outage or impaired service
- Network outage or impaired service (e.g., internet, cellular, NetMotion)
- Critical Systems outage or impaired service

RESPONSIBILITIES

Role	Responsibilities
Executive Sponsor	• Approves the initial and all changes to the policy. • Ensures requisite staffing levels. • Approves metrics, key performance indicators, and service level objectives. • Participates in the Response Team (if appropriate).
Practice Owner	• Establishes and enforces the policy. • Ensures all relevant documentation is current. • Recommends metrics, key performance indicators, and service level objectives. • Determines and recommends changes to the policy. • Approves changes to the process and/or procedures. • Ensures proper training for execution. • Ensures the alignment of the incident policies, process, procedures, and tools with IS' policies and priorities. • Supervises the Incident Management Practice Manager. • Participates in the Response Team (if appropriate).
Practice Manager	• Confirms priority 1 status; creates and owns (parent) ticket and assigns (child) tickets to the appropriate functional team. • Assembles and facilitates the Response Team. • Develops, implements, and maintains the priority 1 Incident Management process and procedural documentation. • Manages internal communication for major, priority 1 Incidents. • Conducts the post incident review (PIR) including the initiator if appropriate; develops and distributes the PIR report. • Advises IS technical support staff of process errors and omissions and ensures proper incident management training is provided via written documentation and training sessions. • Escalates potential risks regarding Incident Management to the Process Owner. • Creates and distributes reports for P1 incident resolution performance against approved metrics, key performance indicators, and service level objectives. • Analyzes Priority 1 Incident Report results and trends; recommends action plans to improve performance and implements approved corrective action. • Recommends process and procedural improvements. • Works closely with the Problem Manager and participates in the Problem Management process (when appropriate).
Service Desk Analyst	• Logs, categorizes, and prioritizes the detected Incident; notifies the Incident Manager immediately. • Recommends process and procedural improvements. • Assigns incoming (child) tickets to the parent ticket for tracking and reporting purposes.
Functional Group Supervisor	• Ensures IM policy, process, and procedures are adhered to by support group personnel. • Ensures assigned support group personnel have the knowledge necessary to resolve the assigned incidents. • Participates in the Response Team (as appropriate). • Participates in post-incident review meetings as appropriate. • Recommends process and procedural improvements.
Communications	• Determines type, frequency, content and medium for external communications (as appropriate). • Manages external communication for major, priority 1 Incidents (if warranted). • Participates in the Response Team (as appropriate). • Consults and assists with internal communications.
Problem Manager	• Participates in the Response Team. • Begins the problem management process immediately (if applicable). • Participates in the post-incident review meeting. • Performs the Incident Manager role as back-up. • Assists incident manager (as appropriate).

Role	Responsibilities
Compliance	• Participates in the Response Team (as appropriate). • Consults and assists with external communications when related to data breach or data related incidents. • Ensures activities align with compliance and regulatory standards.
County Attorney's Office Civil Division	• Participates in the Response Team. • Identifies legal issues. • Liases with outside counsel. ○ Advises on legal requirements and risk mitigation.
Emergency Management Duty Officer	• Participates in the Response Team (as appropriate). • Notifies employee groups of P1 outage and related instructions through Everbridge (as appropriate). • Participates in the post-incident review meeting (as appropriate).
Enterprise Risk Manager	• Participates in the Response Team (as appropriate). • Participates in the post-incident review meeting (as appropriate). • Ensures activities align with risk management policies and standards.

PROCEDURES

See Major – P1 Incident Management procedures under separate cover.

LINKS AND RESOURCES

- Major-1 Incident Management Process
- Major-1 Incident Management Procedures and Work Instructions
- On Call Policy
- Problem Management Policy (5.10.1)
- Problem Management Process
- Problem Management Procedures
- **Security Incident Management Policy (5.9.2)**
- **Security Incident Management Standard**

CONTACTS / SUBJECT MATTER EXPERTS

- Incident Management Sponsor: Chetan Ganatra
- Incident Management Practice Owner: Mike Piram
- Incident Management Practice Manager: Danielle Macy
- Problem Management Practice Manager: Mike Arlt

REVISION HISTORY

Date	Brief description of change
11/10/20	Draft
3/17/21	Finalized content and aligned procedures to policy
3/23/21	Updated post-conditions for process.
3/26/21	Removed watermark, added Policy numbers, corrected typo.

APPROVAL

Rich Christensen
Ramsey County Chief Information Officer
March 26, 2021
Revision History Date Monday, May 17, 2021

‹ Incident Management Priority 2-4 **Back** **Security Incident Management Policy ›**