Policy Title Incident Management Priority 2-4
Department Information Services
Chapter 5
Section 9
Policy 3
Effective Date Monday, August 1, 2022

POLICY STATEMENT

The purpose of this policy is to provide clear guidance regarding Priority 2-4 (P2-4) Incident 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 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 associated with the P2-P4 incident resolution process.
- Continual improvement of the IS Incident Management practice.

APPLICABILITY

All IS personnel who execute and/or manage the priority 2-4 incident management process are to align with this policy.

GENERAL INFORMATION

Policies

- All incidents must be logged in Cherwell.
- Service Desk support hours for priority 2-4 incidents are 7:00 AM-4:30 PM Monday – Friday excluding holidays; support outside of those hours is supplied through the on-call process by the contracted vendor.
- Priority 2-4 incidents shall be resolved in alignment with described roles, responsibilities, processes, and procedures.
- The Incident Manager shall be responsible for internal communication to relevant parties if warranted.
- An incident that is submitted again by the end-user as never being resolved within four business days of the original ticket will be re-opened and measured/reported.
- An incident that is resolved but breaks again within 30 calendar days of the closure of the original incident will be labeled as a "repeat report."
- Communications shall be responsible for external communication to relevant parties if warranted.
- The Service Desk Analyst or Incident Manager will open a Problem record prior to closing the Incident if deemed appropriate.
- All priority 2-4 incidents shall follow the prescribed process unless an exception is approved by the Incident Management Practice Owner.
- If the incident includes a possible data breach, then refer and adhere to the Security Incident Management Policy and Standard.
- The response and resolution time objective for the functional assignee group if the incident is escalated is reflected in the following table.
    - Response time is defined as when the assignee group acknowledges the ticket in the system.
    - Resolution time is defined as when the service returns to "normal" or no longer negatively impacts business operations (e.g., through implementation of an effective workaround).

Priority*	Response Time Objective	Resolution Time Objective
2: High	1 business hour	1 business day
3: Medium	4 business hours	2 business days
4: Low	1 business day	3 business days

*Descriptions and examples for each priority are offered in the Definitions section of this policy.

** "Business hour" and "Business Day" refer to 7:00 AM – 4:30 PM Monday-Friday (excluding holidays). Exception: Infrastructure outages classified as Priority 2 will have a 7X24 "clock."

Process

Priority 2 Incident Management Process

Communication / Notification

Communication will primarily take place through automated email alerts from the Cherwell system and direct communication with application and support personnel.

The Incident Manager will communicate with internal, relevant stakeholders as deemed appropriate for P2 incidents. Communications is responsible for determining the appropriate strategy for external communications if deemed applicable.

Information Services technicians will communicate with internal, relevant stakeholders according to P3-P4 procedures.

Priority	Notification / Communication	Media/Timescale*
2	1. Incident submission	1. IT Service Alert (TSA) withing 60 minutes. 2. ITSA update every 2 hours. 3. ITSA within an hour of resolution.
3-4	1. Incident submission 2. Ticket owner contacts en-user prior to closing ticket 3. Incident resolution.	1. Automated email. 2. Email, phone, chat, in-person. P3- 2 business days. P4- 3 business days. 3. Automated email.

*ITSA for P2 incidents are sent during "normal" Service Desk hours. Cherwell generated updates will continue to go to the initiator.

Metrics/Performance Measures

Priority 2-4 incident management performance will be measured through the following key performance indicators:

- Response time: See table above.
- Resolution time: See table above.
- Communication targets: See table above.
- Volumes by priority.
- Re-opens.
- Repeat reports.
- Process adherence and quality of ticket documentation.

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 Management 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 randomly audit engagement-related documented to ensure adherence to these policies at a minimum of once per 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

Definitions according to (ITIL® v4).

Incident Management – The practice of minimizing the negative impact of incidents by restoring normal service operation as quickly as possible.

Incident - an unplanned interruption to a service or reduction in the quality of that service.

Incident resolution - The workaround or correction that fixes the incident and restores service to its best quality.

Major Incident – an incident with significant business impact, requiring an immediate coordinated resolution. (Further defined in the Major P1 Incident Management Policy)

Impact – The impact is a measure of the effect of an incident, problem, or change on a business process.

Urgency – The urgency is a measure of how long it will be, until an incident, problem or change has a significant impact on the business.

Priority – Priority is a category used to identify the relative importance of and incident, problem, or change. Impact and urgency are used to assign priority. Priority is used to determine the required times for actions to be taken.

Escalation - The act of sharing awareness or transferring ownership of an issue or work item.

Repeat Report (Problem): A ticket resolved, but the same issue reported again within 30 days.

Re-open (Quality): A ticket was resolved but the user contacts within four business days to report that the incident is not resolved. As a result, the ticket is reopened.

This policy pertains to Priority 2-4 Incidents as defined below. Major P1 definitions and examples included as reference. For more information, see the Major P1 Incident Management Policy.

Priority	Definition	Examples
1: Major	"Major" or "priority 1" incidents are defined as technology outages that 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".	**Countywide/Service Team/Department:** • 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 • Malware, virus, evidence of ransomware.
2: High	• Any issue or combination of issues that intermittently interrupt services in a manner such that there is a noticeable detrimental effect on the business or operation of the client. • Mission critical system or service is down or unavailable, but a workaround is available. • Mission critical system or service is working slowly or partially. **Individual (VIP only):** Individual(s) productivity is impacted; cannot perform critical job function(s).	**Service Team/Dept:** • Internal network – intermittent loss/slow. • Partial internet outage. • Wi-Fi. • Citrix. • Email client is down, but O365 mail is available. • Production or infrastructure server down (not test). • Department-specific application down • Security cameras down. * • No server storage space. • Malware alert/malicious activity (multiple related reports.) • VoIP phone or messaging for customer facing call-centers. **Individual (VIP only):** • Laptop/Desktop crashed/rebooted/ (BSOD) and it's impacting a critical job function. • NetMotion doesn't connect. • Malware alert for a privileged account (O or A).

Priority	Definition	Examples
3:Medium	Any issue which results in a loss of function for some of the services and is not critical to the business. A service, or individual is impacted, and no work around is available.	**Service Team/Dept/Multiple Users:** • Server/drive space running low. • Citrix (smaller group). • Security cameras down*. **Individual:** • Device crashed/rebooted (BSOD) not impacting critical job function. • NetMotion unable to connect or quarantined device. • Citrix unable to connect. • MFA (not working after enrollment). • Malware alert/malicious activity. • Escalated phishing incidents.
4: Low	A service, or individual is impacted, but there is low or no impact on productivity.	**Individual:** • Unlock. • Hardware/Peripherals: monitor, keyboard, mouse, speakers, microphone, printer, scanner. • Software: Scripts issue, MS suite, a piece of application functionality. • Access to network shared folder missing/inaccessible. • Aircard not working. • Connecting to home Wi-Fi. • Unable to RDP. • Low memory/disk space. • Server/drive space running low. • Unblock website/application. • MFA (not working after enrollment). • VoIP phone or messaging.

*Depending on public safety

RESPONSIBILITIES

Executive Sponsor

- Approves the initial and all changes to the policy.
- Ensures requisite staffing levels.
- Approves metrics and key performance indicators.

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.

Practice Manager

- Supervises Service Desk Technicians.
- Develops, implements, and maintains the priority 2-4 Incident Management process and procedural documentation.
- Collaborates with functional managers to ensure key activities are optimally resourced.
- Manages internal communication for priority 2 incidents if deemed appropriate; notifies Communications if warranted.
- Escalates potential risks regarding Incident Management to the Process Owner.
- Creates and delivers required Incident reports.
- Recommends process/procedural improvements.

- Works closely with the Problem Manager and participates in the Problem Management process when appropriate.
- Monitors incidents via real-time reports to escalate to functional assignee group manager if response/resolution target time objectives are breached or in danger of being breached.
- Ensures integrity of incident record information before closure; opens Problem record if appropriate.
- Advises IS technical support staff of process errors and omissions and ensures proper incident management training is provided via written documentation and training sessions.

Incident Manager

- Engaged through resolution of active P2 incident.
- Collaborates with functional managers to ensure key activities are optimally resourced.
- Sends internal communication for priority 2 incidents if deemed appropriate; notifies Communications if warranted.
- Escalates potential risks regarding Incident Management to the Process Owner.
- Creates and delivers required Incident reports.
- Recommends process/procedural improvements.
- Ensures integrity of incident record information before closure; opens Problem record if appropriate.

Problem Manager

- Participates in the Technical Bridge.
- Begins the problem management process immediately (if applicable).
- Assists incident manager (as appropriate).
- Recommends process/procedural improvements.

Service Desk Analyst

- Logs, categorizes, and prioritizes the detected Incident.
- Diagnoses and resolves/closes incidents when able.
- Escalates incidents that require functional and/or vendor support.
- Gleans knowledge from incident record details and adds to knowledge base.
- Recommends process/procedural improvements.

Functional Assignee Group

- Acknowledges escalated Incidents within the prescribed time.
- Includes pertinent details regarding Incident resolution in the incident record.
- Provides the incident manager with status updates regarding the resolution process and estimated timeframe for restoral for P2 incidents.
- Provides the incident initiator status regarding the resolution process and estimated timeframe for restoral.
- Collaborates and communicates with vendor resources as applicable.
- Follows documented processes and procedures.
- Recommens process/procedural improvements.
- Develops new or modifies existing Incident Models.
- Confirms incident is resolved with initiator prior to closing the ticket.

Functional Group Supervisor

- Ensures Incident Management 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.
- Monitors incidents via real-time reports to escalate to functional assignee group manager if response/resolution target time objectives are breached or in danger of being breached.
- Recommends process/procedural improvements.

Functional Group On-call staff for after-hours

- Logs, categorizes, and prioritizes the detected Incident.
- Diagnoses and resolves/closes incidents when able.
- Escalates incidents that require functional and/or vendor support.
- Includes pertinent details regarding Incident resolution in the Incident record.
- Provides the incident initiator status regarding the resolution process and estimated timeframe for restoral.
- Provides Service Desk status regarding resolution process and estimated timeframe for restoral, if warranted.
- Follows documented processes and procedures.
- Recommends process/procedural improvements.
- Develops new or modifies existing Incident Models.
- Confirms incident is resolved with initiator prior to closing the ticket.

Communications

- Manages external communication for priority 2 incidents if warranted.

Compliance

- Ensures activities align with compliance and regulatory standards (after receiving reports).

PROCEDURES

See Priority 2 Incident Management procedures and Priority 3-4 Incident Management procedures under separate cover.

LINKS AND RESOURCES

- P1-4 Incident Management Process
- P2 Incident Management Procedures / Work Instructions
- P3-4 Incident Management Procedures / Work Instructions
- P2-3 SIPOC
- On-Call Policy (applicable for P2 incidents)
- **Major P1 Incident Management Policy (5.9.1)**

CONTACTS / SUBJECT MATTER EXPERTS

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

REVISION HISTORY

Date	Brief description of change
Jan. 1, 2021	Draft
July 1, 2022	Updates to the draft

APPROVAL

Chetan Ganatra

Chief Information Officer
Revision History Date Tuesday, October 18, 2022