MAJOR INCIDENT PROCESS

Computing & Telecommunications Services
Wright State University

ITSM-RF/IM Project TeamPrepared by Jonathan R. Jackson
jonathan.jackson@wright.edu

Table of Contents

Prioritization

For purpose of the WSU Major Incident Process, Incidents prioritized as either **"1 – Critical"** or "**2 – High**" will be considered **Major Incidents**. By default, incidents are prioritized by ServiceNow using a matrix based on the Impact and Urgency recorded in the incident record. The matrix is shown below.

		Impact		
		1 – High	**2 – Medium**	**3 - Low**
Urgency	**1 - High**	1 – Critical	2 – High	3 – Moderate
	2 - Medium	2 – High	3 – Moderate	4 - Low
	3 - Low	3 – Moderate	4 – Low	4 - Low

All IT staff are empowered to use their judgment in selecting the appropriate Impact and Urgency for a given Incident, and are empowered to override the Priority of an Incident should they deem the matrix to incorrectly prioritize the Incident. All Incidents where the priority has been overridden will be reviewed by the Service Management Office (SMO).

Impact & Urgency Definitions

Impact

- **High:** Directly impacts teaching and learning, or support services for the entire university or many departments, or imminent public/life safety concern.
- **Medium:** Impacts services provided by a single or few departments
- **Low:** Impacts services provided by an individual or few user(s)

Urgency

- **High:** Core line of business or critical services are affected, or imminent public/life safety concern.
- **Medium:** General university support services are affected
- **Low:** Non-urgent university services are affected

Service Level Targets

The prioritization of Incidents will determine the response and resolution target times, and will determine whether an Incident's targets are using a 24x7 clock or a clock based on university business hours. CaTS' Service Level Targets are listed below.

Unless the university officially specifies otherwise, university business hours will be considered 8:30am-5:00pm Monday - Friday; official university holidays are not considered business hours.

(Goal of all priorities is to achieve response and resolution time 95%)

Priority	Response	Resolution
1 - Critical	**30 continuous minutes**	**4 continuous hours**
2 - High	**90 continuous minutes**	**1 continuous day**
3 - Moderate	1 business day	3 business days
4 - Low	2 business days	5 business days

Note: Some services, such as classroom services will use a different set of Service Level Targets that are more appropriate for the affected service (e.g., 50-minute course meetings)

Incident Manager

CaTS will utilize an Incident Manager role that will be responsible for managing the overall Incident Process to ensure that Incidents are resolved as quickly as possible. The Incident Manager will most often be the Manager of the Service Desk, but may be delegated to others as necessary to cover vacation/sick leave. The role of the Incident Manager may also be delegated to other individuals during an after-hours Major Incident.

The Incident Manager will have the following responsibilities:

- Coordinating Incident Management process, including monitoring and reporting of incidents.
- Be aware of current Incidents in process; detect related Incidents which may be indicative of a more wide-spread problem or an impending Major Incident.
- Coordinate with Tier 2/3 Analysts and Managers when Incidents are escalated to those groups.
- Point of contact for all Major Incidents; will coordinate Incident Resolution activities between various Tiers of Analysts; coordinate communication with CaTS Management, Service Management Office and CaTS Marketing team.
- Ensure workload of Tier 1 Analysts is balanced.
- Conduct Incident reviews as necessary to provide Continual Service Improvement.
- Ensure Closure of Incidents, and follow-up with Users reporting Incidents as not Closed.
- Monitor Incidents to ensure Service Level Targets are achieved.

On-Call Scheduling

CaTS will utilize the On-Call Scheduling application within ServiceNow as the single resource for tracking on-call schedules for each assignment group. Managers of each assignment group will have the responsibility for ensuring the On-Call Schedule is accurate.

Eventually, all CaTS-supported applications, services, and configuration items (“CI” - e.g., servers, network equipment, etc) will be tracked within the Configuration Management Database (CMBD). Each item in the CMDB will be designated a support group in order to assist all CaTS staff in determining the appropriate support group for each item. It is anticipated that

the CMDB will be minimally populated initially and will grow as the department matures its processes and record-keeping.

Major Incident Process

Logging in ServiceNow

The CaTS staff member receiving or recognizing the Incident will record the Incident details within the Incident module in ServiceNow. Once an Incident is recorded in ServiceNow and receives a priority that has been deemed a **Major Incident**, ServiceNow will automatically do the following once 5 minutes has passed since logging the Incident (to prevent notifications as a result of mistaken prioritization):

- Send an email to all CaTS supervisors, managers, directors and CIO (herein referred to as "CaTS Managers").
- If able to be configured, send an SMS message to CaTS Managers. A CaTS Manager may opt-out of receiving SMS with approval of their direct supervisor.
- Send an email to all on-call staff designated within the On-Call Scheduling application at the time the Incident is recorded.
- Send an email to the "Owned By", "Supported By" and "Managed By" users designated in the CMDB for the affected CI.

It is understood that a CaTS staff member may recognize an Incident as a **Major Incident** and may begin working toward resolution prior to logging within ServiceNow. While our goal is to resolve Incidents as quickly as possible, it is expected that all CaTS staff members log an Incident in ServiceNow, or contact the Service Desk (if during staffed hours), as soon as possible so metrics remain accurate and proper notifications and processes can take place.

Contacting On-Call Personnel - Voicemail

The proceeding sections detail processes for contacting On-Call personnel. At each point in the contact process, the individual attempting to contact shall leave a voicemail message when possible.

During Regular University Business Hours

Regular University business hours shall be determined by the official university hours of operation, or 8:30am – 5:00pm if the university does not deem official hours of operation.

Once a **Major Incident** is recognized, the analyst logging the Incident shall inform the Incident Manager of the Incident. The logging analyst will attempt to contact the On-Call Incident Manager on both their office phone and cellphone. The On-Call Incident Manager schedule will be posted within the On-Call Scheduling application in ServiceNow. If the assigned Incident

Manager is unreachable, the logging analyst will attempt to contact other Incident Managers from the On-Call Schedule, even if scheduled during different times. If all Incident Managers are unreachable, the logging analyst shall serve as Incident Manager until an "official" Incident Manager is available. Once the On-Call Incident Manager is available, they will assume the role of Incident Manager for the remainder of the Incident.

Once the Incident Manager is informed of the Major Incident, the Incident Manager will coordinate with applicable Tier 2 or Tier 3 analysts and/or managers to achieve resolution. The Incident Manager will also coordinate with the CaTS Marketing team and CaTS Managers to determine necessary communication with the university community.

The Incident Manager will add the Service Management Office to the Incident's "Watch List" and "Work Notes List" in ServiceNow.

The Incident Manager will contact the Primary On-Call personnel responsible for the affected service on both office phone and cell phone. If the Primary On-Call personnel is unreachable, the Incident Manager will leave voice message; and will wait 10 minutes to attempt again to reach the Primary On-Call personnel. If after a second failed attempt to reach the Primary On-Call personnel, the Incident Manager will attempt to contact the Secondary On-Call personnel (if applicable). If the Secondary On-Call personnel are unreachable and the Incident is prioritized as **1-Critical** the Incident Manager will attempt to contact the manager of the Primary On-Call Personnel and will also contact the manager of the Incident Manager. If the Incident is prioritized as **2-High** the Incident Manager will continue to attempt to contact the Primary and Secondary On-Call personnel in 10-minute increments until the Incident has reached 60 minutes; at which point the Incident Manager will contact their manager and the manager of the On-Call personnel. The Incident Manager will note each contact attempt within the Incident's "Work Notes".

This process shall repeat until the Incident Manager is informed that a staff member capable of resolving the Incident, or their manager, has accepted responsibility of the Incident, at which point the Incident Manager will remain available to coordinate Incident resolution activities with consultation with Tier 2 or Tier 3 analyst or their manager(s).

Once a Major Incident is resolved, the Incident Manager will coordinate with the CaTS Marketing team to determine any necessary communication to the University community, and will assume responsibility of seeing the Incident through the Resolution and Closure process.

After Regular University Business Hours

See **During Regular University Hours** for the definition of business hours.

After business hours, the Help Desk x4827 phone line is staffed either by FTE Staff or Student Help Desk employees, or Data Center Operations staff; however, CaTS Management staff are not working during this time. For the purpose of this section, these staff will be referred to as "Receiving Analyst".

Once the receiving analyst has determined an Incident to be a **Major Incident** they will add the following day's On-Call Incident Manager and the Service Management Office to the Incident's "Watch List" and "Work Notes List" in ServiceNow.

The receiving analyst will attempt to contact the cell phone of the Primary On-Call Personnel for the affected service. If the Primary On-Call Personnel is unreachable, the receiving analyst will attempt to contact the home phone (if applicable) of the Primary On-Call Personnel. If they are still unreachable, the receiving analyst will wait 10 minutes and will again to contact the Primary On-Call Personnel.

If the Primary On-Call Personnel is still unreachable, the receiving analyst will attempt to contact the Secondary On-Call Personnel (if applicable) on both cell and home phones. If the Secondary On-Call personnel is unreachable, the receiving analyst will wait 10 minutes and will again attempt to contact the Primary On-Call Personnel. If still unreachable, and the Incident is prioritized as **1-Critical**, the receiving analyst will attempt to contact the manager of the Primary On-Call personnel, and will repeat this process until either an On-Call Personnel or manager is reached; if the Incident is prioritized as **2-High** the receiving analyst will repeat the process of contacting the Primary or Secondary On-Call Personnel until 60 minutes has passed. Once 60 minutes has passed, the receiving analyst will attempt to contact the manager of the Primary On-Call Personnel. If unreachable, the receiving analyst will repeat this process until either an On-Call Personnel or manager accepts responsibility for the Incident. The receiving analyst will note each contact attempt within the Incident's "Work Notes".

If the contacted On-Call Personnel is able to determine immediately (e.g., still on the phone with the receiving analyst) that another On-Call group is responsible for the Incident, the contacted On-Call Personnel will inform the receiving analyst, at which point the receiving analyst will repeat the contact process for the On-Call Personnel for the group informed by the contacted On-Call Personnel. This process will repeat only two times, at which point the most recently contacted On-Call Personnel is deemed responsible for the Incident. Once an On-Call Personnel has disconnected from the call with the receiving analyst, they will be deemed Incident Manager.

Once either an On-Call Personnel or manager has been deemed the Incident Manager they will coordinate all necessary activities to achieve resolution of the Incident.

Once a Major Incident is resolved, the acting Incident Manager will assume responsibility of seeing the Incident through the Resolution and Closure process. The following day's On-Call Incident Manager, having been on the "Watch List" will be informed of the progress of the Incident, and will coordinate with the CaTS Marketing team to determine any necessary communication to the University community.

If an After Hours Major Incident spills over into the next University business day, that day's On-Call Incident Manager will assume responsibility as Incident Manager once they begin their shift.

Incident Manager & Acting Incident Manager Responsibilities

- Coordinate all Incident resolution activities.
- When possible allow those able to resolve an Incident to focus on Incident resolution. This may require the Incident Manager to play a supportive role by make multiple phone calls to other Tier 2 or 3 analysts needed to assist in resolution, update Work Notes in the Incident record at the direction of Tier 2/3 analysts, etc.
- During an after hours major incident, the "acting" Incident Manager (often a Tier 2/3 analyst who is also responsible for resolving the Incident) may ask another individual involved in the Incident resolution to assume the role of Incident Manager. This most often may occur when the other staff member is playing a lessor role, or is waiting for other tasks to be completed before performing their own tasks.
- If the Incident Manager (or Acting) is able to determine that an Incident may affect other services, even after resolution, the Incident Manager shall be responsible for contacting the On-Call Personnel of those services. An example of this may be (but not limited to) a database server outage that crashes several applications due to their lack of connection to their respective databases.

Responsibilities of All Involved

Team work is essential. Often times a Major Incident cannot be resolved by one individual. The resolution of a Major Incident often involves teamwork and involves multiple groups within CaTS.

Breach of Service Level Targets

If it is apparent that the Major Incident may breach (or has already breached) published resolution Service Level Targets, the Incident Manager shall inform the Service Management Office (SMO). If the SMO concurs with the Incident Manager's assessment of a potential breach, the SMO will call an emergency meeting of CaTS Managers, necessary customer stakeholders, and all-involved analysts to assess the Incident and determine a resolution plan.

The 040 Library Annex conference room shall be the meeting place of the emergency meeting. The emergency meeting will supersede all scheduled meetings in the 040 conference room; however, the emergency meeting will await the conclusion of a meeting already in progress, at which point the 040 Atrium will serve as the meeting place until the 040 conference room is available. The SMO shall be responsible for informing existing meeting organizers of their displacement.

Post-Incident Review

Within 3 business days of a Major Incident's resolution, the SMO shall call a meeting of CaTS Managers, SMO staff, customer stakeholders and all analysts involved in the Incident. The purpose of the meeting shall be:

- Review the Major Incident and its resolution process
- Share lessons learned
- Determine the root cause of the Incident
- Determine actions to prevent a similar Incident from recurring
- Assess the effectiveness of the Major Incident process and discuss potential changes to the process to achieve higher effectiveness.

The post-incident review process will be an open and candid process, focusing on CaTS' ability to provide improved service and warranty to our users. The review meeting and process will not be used to place blame onto an individual or group.