

Consolidated Technology Services

Proposed Approach for Incident Assessment and Response

June 6, 2012

The Severity Level for an incident is initially set by the ‘first responder(s)’, typically the Technician and/or Service Desk, using the definitions below. This is the ‘working’ Severity Level, until confirmed or changed by either the Service Owner, the Incident Management Team, or an Incident Commander designated by the Incident Management Team.

Severity Level 1 (SEV1):

Defined as an incident which causes two or more CTS Vital Services to be unavailable. SEV1 incidents involve a situation that seriously impairs or halts the operations of CTS. Workarounds to restore normal levels of service are not possible or cannot be found in time to minimize the impact on the agency’s business.

Response – The Incident Management Team will assign individuals to, at a minimum, the Incident Command System (ICS) roles of Incident Commander and Public Information Officer. A formal ICS structure will be implemented during all SEV1 incidents. The Incident Commander will work with the Incident Management Team and the Service Owner(s) to fill any additional rolls deemed necessary. The Public Information Officer will ensure that CTS staff, customers, and other key stakeholders are provided updates on the status of the incident.

Status Updates – Default status notification period for a SEV1 incident will be hourly. At any time, the Incident Commander may decide to change the notification schedule. Any change to the schedule will be communicated to affected staff, customers, and all other appropriate parties.

Closure – While an incident may be resolved and systems/applications restored to production levels, a SEV1 incident will not be formally closed without root cause analysis being performed and the results communicated to customers. The initial communication about root cause will take place no later than two weeks after the resolution of the incident. CTS will schedule a meeting to communicate its findings in person to all customers who are interested. During this meeting, a schedule for any necessary further communication will be determined.

Examples of a SEV1 incident:

- Datacenter primary and backup power failure causing an outage to all services.
- Failure of datacenter cooling equipment causing the temperature to rise to unsafe levels for infrastructure which supports vital services.
- A large earthquake which renders CTS buildings uninhabitable.
- Severe weather which causes widespread power outages and limits the ability of CTS staff to commute to work.
- Cyber attack on the state network which results in severely degraded or loss of service.
- Failure of the network core infrastructure in the datacenter.

Severity Level 2 (SEV2):

Defined as an incident which causes two or more CTS Vital Services to be severely degraded or at significant risk of not being available, or a single CTS Vital Service to be unavailable. Workarounds to restore normal levels of service are not immediately known.

Response – The Service Owner will assign a Technical Lead responsible for troubleshooting the problem. The Service Owner will fill the role of the Information Officer, and will ensure that the Service Desk is updated on the status of the incident. If the incident lasts longer than 1 hour with no plan in place for resolution or workaround, the Service Owner will notify the Incident Management Team. They will decide whether a formal Incident Command System (ICS) structure will be implemented. If so, the appointed Incident Commander will work with the Incident Management Team and the Service Owner(s) to fill any additional rolls deemed necessary.

Status Updates – Default status notification for a SEV2 incident will be hourly. At any time, the Service Owner or Incident Commander may decide to change the notification schedule. Any change to the schedule will be communicated to affected staff, customers, and all other appropriate parties.

Closure – While an incident may be resolved and systems/applications restored to production levels, a SEV2 incident will not be formally closed without root cause analysis being performed and the results communicated to customers. The initial communication about root cause will take place no later than two weeks after the resolution of the incident. CTS will schedule a meeting to communicate its findings in person to all customers who are interested. During this meeting, a schedule for any necessary further communication will be determined.

Examples of a SEV2 incident:

- Failure of HRMS infrastructure which causes the service to be unavailable.
- Outage of the phone systems on the Capitol Campus.
- An outage to the state email system.
- Severe weather which limits the ability of CTS staff to commute to work.
- An event causing the evacuation of OB2 or the 1500 Jefferson building.

Severity Level 3 (SEV3):

Defined as an incident which causes a single CTS Vital Service to be degraded or an outage to one or more CTS non-vital services.

Response – The Service Owner will assign a Technical Lead responsible for troubleshooting the problem. The Service Owner will fill the role of the Information Officer, and will ensure that the Service Desk is updated on the status of the incident. If the incident lasts longer than 4 hours with no plan in place for resolution or workaround, the Service Owner will notify the Incident Management Team. They will decide whether to escalate the severity level.

Status Updates – Default status notification for a SEV3 incident will be every 2 hours. At any time, the Incident Commander or Service Owner may decide to change the notification schedule. Any change to the schedule will be communicated to all appropriate parties.

Closure – While an incident may be resolved and systems/applications restored to production levels, a SEV3 incident will not be formally closed without root cause analysis being performed and communicated to customers. The initial communication about root cause will take place within one week of the incident resolution. For SEV3 incidents, CTS will communicate root cause using the Service Desk's standard incident notification procedures. All necessary further communication about root cause will be communicated as it becomes available.

Examples of a SEV3 incident:

- Intermittent failure to deliver email.
- Customers reporting slow response times of traffic entering or traversing the SGN.
- An IBM mainframe customer reporting problems with a CICS region.
- Outage of the state voicemail system..

Severity Level 4 (SEV4):

Defined as an incident which causes one or more CTS non-vital services to be degraded. The service is available to customers but in a limited state.

Response – A Technical Lead (typically ‘on call’) will respond to the incident, and is responsible for ensuring that the incident ticket is updated and all necessary customer communication is complete. If the incident lasts longer than 2 hours with no resolution or workaround, the Technical Lead will inform the Service Owner. The Service Owner will decide whether to escalate the severity level.

Status Updates – There is no default status notification period for a SEV4 incident. The Technical Lead will provide status as they deem appropriate, based on their knowledge of the impact caused by the specific incident.

Closure – SEV4 incidents may or may not require root cause analysis prior to incident closure. The need for root cause analysis will be determined by the CTS technician in collaboration with the impacted customer. If it is determined that root cause analysis is required, the CTS technician will work with the customer to identify an appropriate communication schedule.

Examples of a SEV4 incident:

- A customer reports that their phone does not display who is calling when it rings.
- A customer reports that their emails are not vaulting.
- A customer reports that they cannot log into an IP agent on PBX.

Note: Any incident may be escalated immediately to higher levels or can “stand down” to a lower level based on the nature of the incident (rise or decline in severity or impact). The decision to change the incident severity will be made by the Incident Commander or Service Owner. If a technical lead feels a SEV4 incident should rise to a higher level, they will consult with the Service Owner who will make the final determination.