INCIDENT MANAGEMENT & REQUEST FULFILLMENT PROCESSES

Process Owner: Service Desk Manager

Version: v2.0
# INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

## Document Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Description</th>
<th>Date</th>
<th>Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>Initial Release</td>
<td>Dec-2003</td>
<td></td>
</tr>
<tr>
<td>V3.3</td>
<td>Major update</td>
<td>June-2015</td>
<td></td>
</tr>
</tbody>
</table>
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

CONTENTS

1  Overview of Information Technology Service Management .......................................................... 1
   1.1  ITS Mission ............................................................................................................................. 1
   1.2  ITS Vision .............................................................................................................................. 1
   1.3  ITS Service Management ....................................................................................................... 1
2  Overview of ITIL Service Operations ............................................................................................ 1
   2.1  Access Management (Identity Management) Process* .......................................................... 1
   2.2  Event Management Process* .................................................................................................. 2
   2.3  Incident Management Process* ............................................................................................. 2
   2.4  Problem Management Process* ............................................................................................ 2
   2.5  Request Fulfillment Process* .................................................................................................. 2
   2.6  Applications Management Function ....................................................................................... 2
   2.7  Service Desk Function ........................................................................................................... 2
   2.8  IT Operations Management Function ..................................................................................... 2
   2.9  Technical Management Function ............................................................................................ 2
3  Incident Management & Request Fulfillment Process ................................................................. 3
   3.1  Description ............................................................................................................................. 3
   3.2  Purpose ................................................................................................................................... 3
   3.3  Objectives ............................................................................................................................... 3
   3.4  Scope ....................................................................................................................................... 3
   3.5  Terms of Reference ................................................................................................................. 4
4  Process Flow .................................................................................................................................... 5
   4.1  Incident & Request Identification & Logging .......................................................................... 6
   4.2  Categorization & Priority ........................................................................................................ 8
   4.3  Initial Diagnosis & Escalation .................................................................................................. 8
   4.4  Investigation & Diagnosis ....................................................................................................... 9
   4.5  Resolution & Recovery .......................................................................................................... 9
   4.6  Closure ..................................................................................................................................... 9
   4.7  Tools and Other Deliverables ................................................................................................. 9
   4.8  Communication and Training ................................................................................................. 9
5  Roles and Responsibilities ............................................................................................................. 9
   5.1  Service Desk ........................................................................................................................... 9
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

16.2.1 Procedures: non-SOS Groups, Assignment while creating Case................................. 17
16.2.2 Procedures: non-SOS Groups, Assignment while working Case/Task ......................... 17
16.2.3 Procedures: SOS Groups, Assignment while creating Case ..................................... 18
16.2.4 Procedures: SOS Groups, Assignment while working Case/Task .............................. 19
1 OVERVIEW OF INFORMATION TECHNOLOGY SERVICE MANAGEMENT

1.1 ITS MISSION
Information Technology Services (ITS) is UNCG’s central technology organization, providing computing, communications, and data services. ITS is responsible for planning and management of the transmission and utilization of data, voice, and video, in support of the university's academic and administrative goals. ITS promotes best practices, efficient procurement, and overall cost-effectiveness in the use of IT resources across the entire University.

1.2 ITS VISION
Information Technology Services, with partners on and off campus, uses technology to provide the most cost-effective services and solutions to the UNCG community and our UNC System partners.

1.3 ITS SERVICE MANAGEMENT
IT Service Management (ITSM) is a process-based practice intended to align the delivery of information technology (IT) services with needs of the enterprise, emphasizing benefits to clients. Most ITSM frameworks focus on a process based approach to delivering services. Information Technology Services at UNCG has committed to using the Information Technology Infrastructure Library (ITIL) framework to develop processes that achieve client satisfaction while minimizing costs.

ITIL defines five service lifecycle modules that define processes and functions that are used to manage the services. The service lifecycle modules are:

- Service Strategy
- Service Design
- Service Transition
- Service Operations
- Continual Service Improvement

2 OVERVIEW OF ITIL SERVICE OPERATIONS

The ITIL defined processes and functions within Service Operations are listed below. Asterisks indicate the process or function is defined or implemented within ITS. Asterisk signifies some level of implementation.

2.1 ACCESS MANAGEMENT (IDENTITY MANAGEMENT) PROCESS*
- Process Objective: To grant authorized users the right to use a service, while preventing access to non-authorized users. The Access Management processes essentially execute policies defined in Information Security Management. Access Management is sometimes also referred to as Rights Management or Identity Management.
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

2.2 EVENT MANAGEMENT PROCESS*
- Process Objective: To make sure CIs and services are constantly monitored, and to filter and categorize Events in order to decide on appropriate actions.

2.3 INCIDENT MANAGEMENT PROCESS*
- Process Objective: To manage the lifecycle of all Incidents. The primary objective of Incident Management is to return the IT service to users as quickly as possible.

2.4 PROBLEM MANAGEMENT PROCESS*
- Process Objective: To manage the lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimize the impact of incidents that cannot be prevented. Proactive Problem Management analyzes Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant Problems.

2.5 REQUEST FULFILLMENT PROCESS*
- Process Objective: To fulfill Service Requests, which in most cases are minor (standard) Changes (e.g. requests to change a password) or requests for information.

2.6 APPLICATIONS MANAGEMENT FUNCTION
- Function Objective: The objectives of Applications Management is to see that delivered applications are well designed, resilient and cost-effective, that required functionality is available to achieve the required business outcome, that organization of required technical skills to maintain operational applications in optimum condition and that the resolution of technical failures are speedily diagnosed and resolved.

2.7 SERVICE DESK FUNCTION
- Function Objective: The primary objective of the Service Desk function is to restore the “normal service” to the users as quickly as possible.

2.8 IT OPERATIONS MANAGEMENT FUNCTION
- Function Objective: The objectives of the IT Operations Management function are to: stability of the organization’s day-to-day processes and activities, maintain stability and to diagnose and resolve any IT Operations failures that occur.

2.9 TECHNICAL MANAGEMENT FUNCTION
- Function Objective: Technical Management provides technical expertise and support for the management of the IT infrastructure.
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

3 INCIDENT MANAGEMENT & REQUEST FULFILLMENT PROCESS

3.1 DESCRIPTION
The incident management (IM) and request fulfillment (RM) processes allow communication and tracking of service outages and requests across the organization. These processes define a set of steps to be followed to minimize the impact and duration of service interruption and minimize the time to fulfill requests to attain the highest level of client satisfaction.

3.2 PURPOSE
The purpose of incident management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained. “Normal service operation” is defined as an operational state where services and CIs are performing within their agreed service and operational levels.

The purpose of request fulfillment is to manage the lifecycle of all service requests from the clients.

3.3 OBJECTIVES
The objectives of the incident management process are to:

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents.
- Increase visibility and communication of incidents to business and IT support staff
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
- Align incident management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services

The objectives of the request fulfillment process are to:

- Maintain client satisfaction through efficient and professional handling of all service requests
- Provide a channel for users to request and receive standard services for which a predefined authorization and qualification process exists
- Provide information to users and customers about the availability of services and the procedure for obtaining them
- Source and deliver the components of requested standard services
- Assist with general information, complaints or comments

3.4 SCOPE
The scope of IM includes any event which disrupts or which could disrupt a service. This includes events reported by clients, ITS staff or from monitoring.
The scope of RM includes the process for fulfilling requests for services delivered. This can vary widely depending on the services offered but includes requests from clients, ITS staff or internal ITS request processes.

3.5 Terms of Reference

Definitions of some of the elements of the IM/RM process are included in this section.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>6TECH</td>
<td>Alternate name for Service Desk and implies how to contact Service Desk</td>
</tr>
<tr>
<td></td>
<td>- Phone – 336-256-TECH</td>
</tr>
<tr>
<td></td>
<td>- Web – 6tech.uncg.edu</td>
</tr>
<tr>
<td></td>
<td>- Email – <a href="mailto:6tech@uncg.edu">6tech@uncg.edu</a></td>
</tr>
<tr>
<td>Case or Ticket</td>
<td>In the tracking system, each record containing the information about an incident or request is referred to as a Case or Ticket. This Case is the vehicle by which an incident or request is tracked, assigned to the appropriate ITS resource, reported on, etc. Each Case has a sequential number assigned. The terms “incident”, “case” and “ticket” might be used interchangeably at times, but typically “incident” or “request” refers to the event (the problem, the request, or the inquiry itself) and “case” &amp; “ticket” refers to the tracking database record.</td>
</tr>
<tr>
<td>Client</td>
<td>The individual who is requesting service from ITS or reporting an outage.</td>
</tr>
<tr>
<td>Client Relationship</td>
<td>The relationship between an ITS staff and the client during the fulfillment or resolution of an incident. This process defines standards that must be maintained with the client during the resolution of any incident.</td>
</tr>
<tr>
<td>Contact</td>
<td>The individual that should be communicated with concerning the ticket.</td>
</tr>
<tr>
<td>Documentation</td>
<td>In each step of the process, it is important that clear, accurate and complete documentation is performed. Documentation for an incident includes information that is input in Remedy, including all mandatory fields as well as Work Log entries and attachments associated with the Remedy Case for that incident. This information is critical for tracking issues and incidents and for developing a knowledge base of problems and solutions experienced by the ITS</td>
</tr>
</tbody>
</table>
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

<table>
<thead>
<tr>
<th>DTS</th>
<th>community (see complete documentation guidelines in 4.1 Documentation).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>A team or group of people and the tools or other resources they use to carry out one or more processes or activities.</td>
</tr>
<tr>
<td>Incident or Request</td>
<td>In the context of the ITS IM/RM process, an incident is an inquiry, problem report or any other request for assistance, made by a member of the UNCG client community to ITS.</td>
</tr>
<tr>
<td>Process</td>
<td>A structured set of activities designed to accomplish a specific objective.</td>
</tr>
<tr>
<td>Process Manager</td>
<td>A role responsible for the operational management of a process.</td>
</tr>
<tr>
<td>Process Owner</td>
<td>The person who is held accountable for ensuring that a process is fit for purpose.</td>
</tr>
<tr>
<td>Service Desk</td>
<td>A functional unit made up of dedicated staff responsible for dealing with a variety of service events.</td>
</tr>
<tr>
<td>Service Owner</td>
<td>A role responsible for managing one or more services throughout the services’ entire lifecycle.</td>
</tr>
</tbody>
</table>

4 GUIDING PRINCIPLES – STANDARDS

The following are the standards for incident management and request fulfillment.

1. All incidents and requests must go through the Service Desk, providing clients with a single point of contact.
2. Summaries for tickets must be selected from a dropdown list which define the support group assigned, the categorization, and the service impacted.
3. Summaries may have additional information required in the Notes field.
4. When applicable, tickets will have the CI impacted related.
5. Requests for additional summaries will be submitted as a request and must define the support group responsible and the categorization.
6. Incident reporting and requests that use 6TECH web (Service Catalog) will have automatic routing which has been vetted through the Service Desk.
7. All incidents and requests must be logged, prioritized and solutions recorded in Remedy Incident Management.
8. One standard Incident Management and Request Fulfillment process is defined and used to support all ITS clients.
9. The Service Operations & Support group and the Service Desk are the conduit of communication of any degradation of service. For any mass communication required these groups partner with ITS Doc & Comm group to communicate with clients and ITS staff.
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

10. All ITS staff are required to manage, track, escalate, close and communicate status of all incidents and requests to clients based on Service Level Targets.

11. Closure of tickets is dependent on validating with the user that the incident or request has been resolved and service is restored or available.

12. Ownership of tickets will be remain with the support group assigned after initial escalation unless the request reassign process is followed.

13. Once a priority 1 or priority 2 incident has been validated by Service Operations & Support, escalation and communication protocols for high-priority incidents will be initiated and managed by the Enterprise Incident Management team.

14. Tasks can be created to obtain further assistance with a ticket but must be assigned to a group and not a member of the group.

15. Documentation should be concise, clear, complete, correct, and clean.

16. Anyone viewing the Case should be able to discern:
   a. the problem
   b. the current status
   c. work steps towards resolution being attempted
   d. group and owner of the ticket
   e. the exact resolution

5  PROCESS FLOW

5.1 INCIDENT & REQUEST IDENTIFICATION & LOGGING

Incidents/Requests may be identified by clients, ITS staff, or automated systems. There are several input methods for incidents or requests. Incident identification is used for tracking, assisting in finding solutions and compiling historical information for future use and reporting. Incidents must be fully logged and date/time-stamped, regardless of input source. This retains a full historical record. Below are steps to take to identify and log each type of incident or request. Once these two steps are complete move to the next phase of the process flow.

5.1.1 Phone call to the Service Desk or walk-in to TSC
1. Verify issue or service exists
2. Create a new ticket
3. Identify client and record required client information
4. If the calling individual is different from the client, record the requested for information
5. Review open cases for client and verify that this is a new incident/request – if it is not new then do not save this ticket and continue to work on the existing ticket – see section Investigation & Diagnosis
6. Verify client location and note if location is different
7. Verify location of incident or request and note if location is different
8. Gather description of issue
9. Verify with client that you understand the issue
10. Take steps to validate or replicate the interruption
11. Gather any data about the issues (screenshots, descriptions)
12. Determine if email is concerning an incident (User restoration) or a request (User request) and note in case
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

13. Select the Reported Source of the ticket

5.1.2 Email – Incident or Request
1. Create a new ticket
2. Identify client and record required client information
3. If the email is from a different from the client, record the contact information
4. Review open cases for client and verify that this is a new incident/request – if it is not new then do not save this ticket and continue to work on the existing ticket – see section Investigation & Diagnosis
5. If email states any differences about client information note differences
6. If email states location of incident or request is different note differences
7. Copy email header into Notes field
8. Copy text of email into Notes field below header
9. Determine if email is concerning an incident (User restoration) or a request (User request) and note in case
10. Select the Reported Source of the ticket

5.1.3 Form - Request
1. Create a new ticket
2. Identify client and record required client information
3. If the form indicates a contact different from the client, record the contact information
4. Review open cases for client and verify that this is a new incident/request – if it is not new then do not save this ticket and continue to work on the existing ticket – see section Investigation & Diagnosis
5. If email states any differences about client information note differences
6. If email states location of incident or request is different note differences
7. Copy email header into Notes field
8. Copy text of email into Notes field below header
9. Determine if email is concerning an incident (User restoration) or a request (User request) and note in case
10. Select the Reported Source of the ticket

5.1.4 Direct Entry – ITS Staff or DTS
1. Create a new ticket
2. Record required client information
3. Review open cases for client and verify that this is a new incident/request – if it is not new then do not save this ticket and continue to work on the existing ticket – see section Investigation & Diagnosis
4. Determine if this is concerning an incident (User restoration) or a request (User request) and note in case
5. Select the Reported Source of the ticket

Now that identification and logging are complete proceed to Categorization & Prioritization
5.2 Categorization & Prioritization
Client information and notes have been entered into the new ticket. The next step is to categorize and prioritize the ticket. See the section Category below for a complete explanation of defining the category. See the section Prioritization below for a complete explanation of defining priority.

Assigning a category and priority will determine how an incident is handled in the remainder of the process.

5.2.1 All ticket initiators
1. Select the summary that most closely matches the information in the ticket – the summary will include the category and escalation information.
2. Add additional information to clarify the summary (up to 60 characters).
3. Select the CI that is impacted
4. Select the priority based on the below chart

<table>
<thead>
<tr>
<th>Priority Code</th>
<th>Examples</th>
</tr>
</thead>
</table>
| 1 - Critical  | • Critical service interruption impacting multiple buildings.  
                • A mission critical application service (i.e. Banner, Canvas or email) is not available. |
| 2 – High      | • Two or more users are unable to perform critical business functions Critical business function(s) not able to be performed (e.g. network problems isolated to a particular room or building, primary group-specific application not available)  
                • Instructor station in lab not functioning |
| 3 - Medium    | • One user is unable to perform critical business functions (e.g. workstation hardware or operating system problem). Lab workstations are an exception to this rule: instructor station problems = Priority 2, individual lab workstations = Priority 4  
                • Two or more users are experiencing a problem that does not impact critical business functions (e.g. printer problems when another printer is available, problems with non-critical desktop applications) |
| 4 – Low       | • One user is experiencing a problem that does not impact critical business functions (e.g. printer problems when another printer is available, problems with non-critical desktop applications)  
                • Client inquiries such as “how-to” or application-specific support questions  
                • One lab workstation  
                • Routine requests that have an associated pre-determined workflow (e.g. Lab scheduling, project requests, documentation) is not functioning |

5.3 Initial Diagnosis & Escalation
Incident or request has identified, logged, categorized and prioritized. The next step is to identify symptoms and perform initial diagnosis using diagnostic scripts, known error information and documentation. If a resolution can be found, determine steps to be performed, log the steps taken and skip to resolution & recovery.

Determine if escalation is needed. See Functional and Hierarchical Escalation for details.
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

5.3.1 All ticket initiators
1. If ticket is Priority 1 or 2, following Emergency Incident Management procedure.
2. If ticket can
   - Create or update incident activity log and communicate status.
   - Adjust incident categorization if necessary
   - Determine incident prioritization
   - Contact client if more information is needed
   - Resolve if possible, otherwise escalate to appropriate support group.

5.4 INVESTIGATION & DIAGNOSIS
Each support group involved with an incident will investigate and diagnose and will maintain a detailed record of any actions taken to try to resolve or recreate the incident.

5.5 RESOLUTION & RECOVERY
When a resolution is identified, it should be applied and tested. An incident must be updated with detailed information.

5.6 CLOSURE
Service Desk Analyst must confirm the resolution and client satisfaction before incident closure. Incident categorization should be checked and confirmed. If categorization is incorrect, it should be updated so that the incident information is correct. Ensure that incident record is fully documented before closure.

5.7 TOOLS AND OTHER DELIVERABLES
The tool of choice to facilitate IM and RM is BMC Remedy software. This manual describes the ITS IM/RM model and specific IM/RM processes and associated procedures. Details of how to use the BMC Remedy software are described in the Remedy user guide.

5.8 COMMUNICATION AND TRAINING

6 ROLES AND RESPONSIBILITIES

6.1 SERVICE DESK
- Tier 1 support
- Logging the incident in the call log
- Performing the initial Incident diagnostics
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

- Requesting technician support when required through functional or hierarchical escalation
- Owning, monitoring and communicating
- Updating records (call log, incident sheet) with the resolution
- Closing incidents
- Progressing any follow up action (for example, following through into problem management)

6.2 SERVICE OPERATIONS

- Managing the communication between monitoring and IM

6.3 TECHNICAL RESOURCE – TIER 2 SUPPORT - (ESCALATION POINT)

- Owning, monitoring and communicating
- Updating records (call log, work information)
- Requesting technician support when required through functional or hierarchical escalation
- Closing incidents assigned to them
- Progressing any follow up action (for example, following through into problem management)
- Verify summary and categories are correct, if not make correction
- Record any activity performed in the work notes
- When work from an additional support group is required, assign a task to the appropriate support group and provide the reason in the work notes
- Recording the resolution, succinct but descriptive of work completed (“Done”, “Completed” is not descriptive)
- Confirm whether the Incident is similar to or a repeat of another active Incident
- If incidents are erroneously linked, unlink them
- If incidents should be linked, link them
- Communicate regular updates to the user

6.4 SUPPORT GROUP MANAGER

- Accountable for the activities and resources required to resolve all escalated incidents, assigned requests and tasks per the Service Level Management targets
- Accountable for providing up-to-date on call contact details to appropriate parties
- Accountable for providing up-to-date information on group members
- Accountable for ensuring that clients receive updates on open tickets assigned to the group based on the Service Level Management targets
- Act as a further escalation point for the team
- Monitor the team’s queue and assigns incidents, requests and tasks to the appropriate individuals within their team
- Ensure that work on incidents, requests and tasks is completed with agreed timeframes and in accordance with Service Level Management targets
- Liaise with other support group managers to ensure handover, continuity and consistency
- Ensure all tickets have current status updates
- Review incidents, requests and tasks aging reports and ensures team is working on the tickets
- Work with Incident Management Process Owner to develop/update summaries
6.5 **Process Owner – Incident Management & Request Fulfillment**
- Sponsor, design and provide change management to the process and its metrics
- Define the process strategy and assist with the process design
- Ensure that appropriate process documentation is available and current
- Define appropriate policies and standards to be employed throughout the process
- Periodically audit the process to ensure compliance to policy and standards
- Periodically review the process strategy to ensure that it is still appropriate and change it if required
- Review opportunities for process enhancements and for improving the efficiency and effectiveness of the process
- Sponsor and pursue improvements to the process
- The process owner is AVC for Systems and Networks

6.6 **Process Manager – Incident Management & Request Fulfillment**
- Work with the process owner to plan and coordinate all process activities
- Manage resources assigned to the process
- Work with service owners and other process managers to ensure the smooth running of services
- Monitor and report on process KPIs
- Identify improvement opportunities
- Make improvements to the process that are sponsored by the process owner
- Develop and maintain the incident management process and procedures.
- Validate new categories in a timely manner
- The process manager is the Service Desk Manager

6.7 **Service Owners**
- Analyze Incident and Request reports and trends
- Identify and sponsor improvement initiatives for how their service handles Incidents and Requests
- Accountable for providing input into the Incident and Request summaries and categorization scheme

6.8 **RACI Chart**
The RACI chart below shows the roles and responsibilities as described above in a different form. For this chart the letters RACI are defined as:
- R Responsibility
- A Accountability
- C Consult
- I Informed
7 INCIDENT TYPE

ITS has implemented IM and RM using the same components of BMC Remedy tool. The differentiator for users being an incident is a service outage and a request is asking for a service (or change in a service). For logging event management incidents, the differentiator is a service outage or service threshold being met. Each ticket will display the incident type selected from one of the four types of incidents listed below.

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Service Restoration</td>
<td>A user is experiencing a service outage</td>
</tr>
<tr>
<td>User Service Request</td>
<td>A user is requesting a service, a change in a service or asking for information</td>
</tr>
<tr>
<td>Infrastructure Restoration</td>
<td>A service is experiencing a service outage</td>
</tr>
<tr>
<td>Infrastructure Event</td>
<td>A service has reached a threshold and should be reviewed</td>
</tr>
</tbody>
</table>

8 SUMMARY

The Summary of an Incident will be selected from a predetermined list generated by the Incident Type. Select the Summary that best fits the Incident. You may add a Summary Addition if a brief description is required. NOTE: The Summary Addition does not replace the Notes field. The Notes field will still be used for a complete description of the Incident.

Summary: A brief description of the Incident.

Summary Addition: A brief addendum to the Summary (60 characters).
The prioritization of a ticket is based on the impact of the incident or request and the urgency of the incident or request. These factors are based on defined criteria which may not match the feeling that a client expresses.

Impact is based on the effect on business criticality, defined service level agreement and generally has components of finance, legislation, regulation, security or reputation.

Urgency is based on the extent to which the resolution or fulfillment can bear delay.

The combination of these two factors will determine the priority.

The priority is assigned by the business not by the client.

Each ticket will be assigned a priority based on guidelines listed below. Any ticket that is determined to be a priority 1 (P1) or priority 2 (P2) will be forwarded to the Enterprise Incident Management (EIM) process.

<table>
<thead>
<tr>
<th>Priority Code</th>
<th>Examples</th>
</tr>
</thead>
</table>
| 1 - Critical  | • Critical service interruption impacting multiple buildings.  
                • A mission critical application service (i.e. Banner, Canvas or email) is not available. |
| 2 - High      | • Two or more users are unable to perform critical business functions. Critical business function(s) not able to be performed (e.g. network problems isolated to a particular room or building, primary group-specific application not available)  
                • Instructor station in lab not functioning |
| 3 - Medium    | • One user is unable to perform critical business functions (e.g. workstation hardware or operating system problem). Lab workstations are an exception to this rule: instructor station problems = Priority 2, individual lab workstations = Priority 4  
                • Two or more users are experiencing a problem that does not impact critical business functions (e.g. printer problems when another printer is available, problems with non-critical desktop applications) |
| 4 - Low       | • One user is experiencing a problem that does not impact critical business functions (e.g. printer problems when another printer is available, problems with non-critical desktop applications)  
                • Client inquiries such as “how-to” or application-specific support questions  
                • One lab workstation  
                • Routine requests that have an associated pre-determined workflow (e.g. Lab scheduling, project requests, documentation) is not functioning |

10 SERVICE LEVEL TARGETS

All tickets are subject to the service level targets which are defined based on the priority of the ticket. The three standards are:

<table>
<thead>
<tr>
<th>Service Level Target</th>
<th>Description</th>
</tr>
</thead>
</table>
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

<table>
<thead>
<tr>
<th>Case Acceptance Standards</th>
<th>Allowed time lapse before a ticket should be assigned to an individual and work begin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Contact Standards</td>
<td>How frequently a client should be contacted &amp; a client contact entry should be made</td>
</tr>
<tr>
<td>Case Update Frequency Standards</td>
<td>How frequently a ticket should have a status update – a meaningful work log entry – to determine the status the case</td>
</tr>
</tbody>
</table>

Details of determining whether or not the processing of a ticket is in compliance with these standards and what monitoring steps are taken in association with these standards are also included. Compliance to these standards is expected on all ITS incidents and service requests.

10.1 CASE ACCEPTANCE STANDARDS
Tickets that are not resolved at first client contact will be assigned to a group. The Case Acceptance Standard refers to the allowed time lapse before a ticket should be assigned to an individual and work begin. Any case with functional escalation from the Service Desk or transferred to a different group via the reassign process is subject to the Case Acceptance Standards. All tasks are subject to the Case Acceptance Standards. Elapsed time is business hours; ie the clock is only ticking M-F 8am – 5pm.

To meet the Case Acceptance Standards the case must be assigned to an individual. Failure to meet standards results in notification sent to Group Manager at listed frequency.

The elapsed time permitted depends on the Priority level of the Case as shown below:

<table>
<thead>
<tr>
<th>Case Acceptance Standards</th>
<th>Acceptance Standard in Elapsed Business Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Acceptance Standard in Elapsed Business Time</td>
</tr>
<tr>
<td>1 - Critical</td>
<td>15 minutes</td>
</tr>
<tr>
<td></td>
<td>Failure notification frequency: 15 minutes</td>
</tr>
<tr>
<td>2 - High</td>
<td>30 minutes</td>
</tr>
<tr>
<td></td>
<td>Failure notification frequency: 30 minutes</td>
</tr>
<tr>
<td>3 - Medium</td>
<td>4 business hours</td>
</tr>
<tr>
<td></td>
<td>Failure notification frequency: 1 business hour</td>
</tr>
<tr>
<td>4 - Low</td>
<td>9 business hours</td>
</tr>
<tr>
<td></td>
<td>Failure notification frequency: 1 business hour</td>
</tr>
</tbody>
</table>

10.2 CLIENT CONTACT STANDARDS
Tickets that are not resolved at first client contact require frequent contact with the client to keep them apprised of the progress on their request. These standard refer to the allowed time lapse between each contact with a client. Elapsed time is business hours; ie the clock is only ticking M-F 8am – 5pm.

To meet the Client Contact Standards the client must be contacted via approved mechanisms and that contact recorded in the Work Info. Failure to meet standards results in notification sent to Group Manager at listed frequency.

Acceptable forms of contact are based on priority.
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

The elapsed time permitted depends on the priority level of the case as shown below.

<table>
<thead>
<tr>
<th>Client Contact Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
</tr>
<tr>
<td>-----------</td>
</tr>
</tbody>
</table>
| 1 - Critical | • Initial contact: within 15 minutes  
• Ongoing: every 2 hours  
• Failure notification frequency: every 30 minutes |
| 2 - High | • Initial contact: within 30 minutes  
• Ongoing: every 4 hours  
• Failure notification frequency: every hour |
| 3 - Medium | • Initial contact: within 4 hours  
• Ongoing: every 2 business days  
• Failure notification frequency: once a business day |
| 4 - Low | • Initial contact: within 8 hours  
• Ongoing: every 3 business days  
• Failure notification frequency: once a business day |

Notes:
Exemption: A Case may be exempted from the Client Contact Standards if the date of next expected action on the Case is documented within the ticket (using the field “Next Activity”, which requires a Client Contact entry to be made)

10.3 CASE UPDATE FREQUENCY STANDARDS

Tickets that are not resolved at first client contact require frequent updates so that the status and progress is noted. These standards refer to the allowed time lapse between each update to the case. Elapsed time is business hours; ie the clock is only ticking M-F 8am – 5pm.

To meet the case update standards an entry must be made in the work info. This entry can be made by either the assignee or any member of the group. The required frequency depends on the priority level of the case as shown below:

<table>
<thead>
<tr>
<th>Case Update Frequency Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
</tr>
<tr>
<td>----------</td>
</tr>
</tbody>
</table>
| 1 - Critical | • Update frequency: every 60 minutes  
• Failure notification frequency: every 60 minutes |
| 2 - High | • Update frequency: every 4 hours  
• Failure notification frequency: every 4 hours |
| 3 - Medium | • Update frequency: every 2 business days  
• Failure notification frequency: once a business day |
| 4 - Low | • Update frequency: every 3 business days  
• Failure notification frequency: once a business day |
11 ADDITIONAL INFORMATION CONCERNING GUIDELINES

Additional details of guidelines are listed below.

11.1 DOCUMENTATION

All information that is recorded in a ticket including Description, Work Log entries, and Solution Details, is considered “documentation” for the incident and should follow the guidelines below-

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concise</td>
<td>As brief as possible while including all information necessary to describe situation</td>
</tr>
<tr>
<td>Clear</td>
<td>No ambiguity; no cryptic explanations or nonstandard shorthand or abbreviations; correct spelling and grammar.</td>
</tr>
<tr>
<td>Complete</td>
<td>Include problem description and detailed steps taken as to resolution – will facilitate ability to resolve future similar problems</td>
</tr>
<tr>
<td>Correct</td>
<td>Accuracy is critical</td>
</tr>
<tr>
<td>Clean</td>
<td>Language is nonjudgmental and professional. Call information should be able to be read by either the original client or anyone else in the UNCG client community without causing controversy.</td>
</tr>
</tbody>
</table>

Ideally, a person with no prior knowledge of a situation should be able to understand the problem and perform its solution simply by reading the Description and Solution Details. These fields must clearly and quickly convey relevant information in a professional manner. "Professional" means that the writing would not be an issue if it were read in a meeting with the client, the author and/or ITS management. Attention must be paid to spelling, grammar, accuracy and tone.

**GOALS FOR CASE DOCUMENTATION**

Documentation should be **concise, clear, complete, correct, and clean**.

Anyone viewing the Case should be able to discern:
- the problem
- the current status
- work steps towards resolution being attempted
- group and owner of the ticket
- the exact resolution
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

11.2 HELP DESK CASE AND TASK ASSIGNMENT
A combination of Cases and Tasks will be used for Remedy service requests. The following policies are in place for how “Individual” and “Group” assignments for Cases and Tasks will be made.

- Assignment to “Individual”: Staff can assign Case to another member of their Group, but not to a member of another Group. (Each Group can determine procedures for assigning tickets within their Group.)
- Assignment to “Group”: Staff can assign Case to their own Group (according to internal Group procedures), but not to any other Group, unless they are the Submitter (creator) of the Case.*
- If a Case requires work to be done by multiple Groups, the Case will remain assigned to the primary group and Tasks will be assigned from that Case to any other Group working the issue.
- Mis-assigned Cases will be handled via the Request Reassignment function; SOS management will be responsible for approval and execution of the reassignment request for mis-assigned Cases.

Procedures for these policies will vary between SOS groups (Service Desk, Service Operations, and EIM) and non-SOS groups.

11.2.1 Procedures: non-SOS Groups, Assignment while creating Case

Scenario 1 – You create and submit a Case that another member of your Group will handle.

1. Create and save the Case. System will assign the Case to you and your Group.
2. Change Individual assignment to another Group staff and Save. Case will be reassigned to that staff.

Scenario 2: You create and submit a Case that you believe should be handled by Group “X” (not your Group).

Create and save the Case. System will assign the Case to you and your Group.

1. Change Group assignment. Case will be assigned to that Group.
2. This is the only time a non-SOS staff can assign a Case to another Group.

11.2.2 Procedures: non-SOS Groups, Assignment while working Case/Task

Scenario 1: You have been assigned a Case by your Group manager (or other member of Group, as dictated by internal Group procedures). You complete some work on the Case and, at some point, determine that another Group (Group “X”) needs to work on it. You remain the Case “assignee” and create a Task for the next Group.
INCIDENT MANAGEMENT AND REQUEST FULFILLMENT PROCESSES

1. Create a Task and assign it to Group “X”. Include the details of the work that you are requesting.
2. Group “X” manager (or other Group staff, as permitted by internal Group procedures) assigns Task to Group individual.
3. Task assignee completes work and closes Task.
4. Complete any other work required to complete the Case, enter the resolution and close the Case.

Scenario 2 ("Misrouted Cases") : You have been assigned a Case by your Group manager (or other member of Group, as dictated by internal Group procedures). You immediately determine that the Case should have been initially assigned to another Group. The Case will be flagged as “mis:assigned” and directed to TSC for remediation.

Select Request Reassignment.

Complete prompts to indicate to which Group you believe the Case should have been assigned and why you believe the Case was mis-assigned.

SOS management will be notified about the mis:assigned Case, verify the need for reassignment, and assign the Case appropriately. NOTE: Until SOS management assigns Case to someone else, the Case is still assigned to you.

11.2.3 Procedures: SOS Groups, Assignment while creating Case

Scenario 1 – You create and submit a Case that another member of your Group will handle.

1. Create and save the Case. System will assign the Case to you and your Group.
2. Change Individual assignment to other Group staff and Save. Case will be reassigned to that staff.

Scenario 2 – You create and submit a Case that you believe should be handled by non-SOS Group.

1. Create and save the Case. System will assign the Case to you and your Group.
2. Change Group assignment. Case will be assigned to that Group.

Or

1. As creating Case, choose appropriate Group for assignment and Save.
11.2.4 Procedures: SOS Groups, Assignment while working Case/Task

Scenario 1 – You have been assigned a Case by your Group manager (or other member of Group, as dictated by internal Group procedures). You complete some work on the Case and, at some point, determine that another Group (Group “X”) needs to work on it. You remain the Case “assignee” and create a Task for the next Group.

1. Create a Task and assign it to Group “X”. Include the details of the work that you are requesting.
2. Group “X” manager (or other Group staff, as permitted by internal Group procedures) assigns Task to Group individual.
3. Task assignee completes work and closes Task.
4. Complete any other work required to complete the Case, enter the resolution and close the Case.