1. **Purpose**  
The following outage and change management procedures are intended to provide centralized scheduling, tracking and communication of planned and unplanned outages to Information Technology (IT) infrastructure. The procedures apply to any outage or planned change to current (in production) central Information Technology (IT) infrastructure, including but not limited to servers, critical hosting and operations services (such as E-Mail, Web, DNS, DHCP, and databases) and any and all network infrastructure and architecture.

2. **Outage / Change Management Procedure Overview**  
   a. Unplanned Outages
      i. Classified as severity 3, 4 or 5 according to matrix in section 2.
      ii. Opened (via web or email) by primary contact person
      iii. Details of outage to be contained in a web-based outage database or manually transmitted by email (outage@colby.edu)
      iv. Communication, notification and status reports issued based on severity, as outlined in section 4.
   b. Planned Outages/changes
      i. Classified as severity 0, 1 or 2 according to matrix in section 2.
      ii. Opened (via web or email) by primary contact person (individual who will be doing the work)
      iii. Presented and discussed at appropriate change management meeting, if applicable
      iv. Communication, notification and status reports issued based on severity, as outlined in section 5.

3. **Outage Classification and Response Matrix**  
The following matrix is used to assign a numerical severity value to an outage or planned event based on the conditions, services and/or number of clients involved. Each level of severity dictates a certain response in terms of notification to other personnel.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Conditions</th>
<th>Response/Notification</th>
</tr>
</thead>
</table>
| 5        | Unplanned outage
          | Critical service is down/unreachable
          | Many high-priority services are down/unreachable | urgent notification (voice bomb, global or targeted email, web) |
| 4        | Unplanned outage
          | Critical service is degraded
          | High-priority service is down
          | Multiple medium/low priority services down | Notification determined by support (voice bomb, global or targeted email, web) |
| 3        | Unplanned outage
          | Multiple high-priority services degraded
          | Redundant services down
          | Medium/low priority services down | Standard notification (targeted email, web) |
| 2        | Planned outage on critical services | Public notification (targeted email or web, as determined by support) |
| 1        | Planned outage on non-critical services or degradation of critical service | Public notification (web), as needed/determined by support |
| 0        | Planned work on low priority or redundant services | No notification – only outage form |
4. Outage Management and Status
   a. Outages will be submitted and queried via a web portal:
      i. [http://www.colby.edu/administration_cs/its/office/outage/index.cfm](http://www.colby.edu/administration_cs/its/office/outage/index.cfm)
      ii. If the web is unavailable, the primary contact will resort to email (via outage@colby.edu)
      iii. If email is unavailable, the primary contact will use the telephone to communicate with support desk(s)
   b. All outages (planned or unplanned) will have a status of:
      i. Proposed
      ii. Scheduled/Approved
      iii. In Progress
      iv. Monitoring
      v. Closed
      vi. Cancelled / Denied
   c. Change Management (CM) meetings occur at least once per week
      i. Monday mornings at 10AM
      1. emergency/overflow: Wednesday mornings at 9AM
      ii. Planned work should be submitted at the CM meeting two weeks before the scheduled outage
         1. Urgent planned work can be submitted a minimum of one hour before a CM meeting
         2. Emergency work can be submitted with approval from the director of support or support designate
      iii. Outages from the prior week will be reviewed at the Monday CM meeting

5. Procedure for Unplanned Outage (severity 5/4/3)
   a. Detection, confirmation, classification
      i. Problem is detected
         1. Detected on monitoring (see section 8c and 8d)
         2. Detected by service department (ITS or other trusted department)
         3. Confirmed complaints from user community
      ii. Outage has gone on for longer than 2 minutes or is of a highly critical system or service (as determined by support or ITS department)
      iii. Outage is classified by severity (see section 3)
   b. Communication
      i. Servicing department/individual (whoever is going to work on the problem)
         1. Phone support desk (if unanswered, contact director) to notify of outage
         2. Open outage event via web form (if unavailable, contact support)
            a. Start time/date
            b. Affected clients/services
            c. Estimated downtime (if available)
            d. ITS internal contact person (who will be providing updates, who support should contact with questions)
               i. Secondary internal contact person if relevant
      ii. Support Center communicates status to users/community based on information provided by servicing department/person
         1. Method depends on classification
            a. Severity 5 = urgent notification – voice, email, phone as determined by support
            b. Severity 4 = notification by email or web
         2. Severity 3 = notification if necessary
      iii. Updates based on severity (provided directly to support or via outage web)
         1. Severity 5 – updates at least every 30 minutes
         2. Severity 4 – updates at least every 60 minutes
         3. Severity 3 – updates as needed
   c. Completion / Closing
i. ITS internal contact changes outage status via web (or uses phone if web unavailable)
   1. Outage end time
      a. Monitoring period determined by primary contact
   2. Resolution/summary (what caused the outage, what was done)

ii. Support Center communicates status to users/community based on information provided by servicing department/person

iii. Follow-up discussed at the next CM meeting (Mondays, 10AM) unless otherwise determined by support or ITS administration

6. Procedure for Planned Outage (severity 2/1/0)
   a. Planned outages must be coordinated and carried out under the following conditions
      i. Work has been summarized and submitted (via web interface)
         1. Start date/time
         2. End date/time
         3. Length of outage (disruption(s))
            a. What is expected
         4. Title and description of work
         5. Scope of work
            a. What services are affected
            b. What users/clients are affected
         6. Primary contact (who is doing the work)
         7. Secondary contact (backup)
      ii. Work is announced at the weekly change management meeting (Monday 10AM)
         1. Work can be pre-approved pending changes
      iii. Work is conducted during established work window
         1. Planned work window is between 1AM and 7AM Wed. mornings
            a. Planned outages (of severity 1 or 2) are expected to take place at some point during the weekly window
            b. Exceptions to the work window (any of the following)
               i. Outage is severity 0 (Informational), non-impacting
               ii. Affected group(s) have been previously notified and approved of outage
                  1. Prior notification must be noted in the outage
               iii. Work is completed on a green day. Each calendar day should fall under three categories, color coded as:
                  1. RED: No work allowed (such as during exams)
                  2. GREEN: Work window not applied. (campus is closed or on holiday/break)
                  3. WHITE (or none): Normal work window and outage policy in effect
            iv. Notice has been given to the user community based on submitted summary
               1. Severity 2 (critical) – requires public notification
                  a. Notice of work within the work window is only required to be posted on the outage web site
               2. Severity 1 (non-critical) – automatically posted to outage web
      b. Completion / resolution of planned outage
         i. If work is completed as expected, the event ticket should be updated with
            1. completion time/date
            2. actual downtime (did work go as planned)
            3. any additional notes
            4. follow-up discussion at next regular event planning meeting
ii. If work is not completed as expected, primary contact may continue the work (if non-impacting) or close the outage (with explanation) and track further changes under a new outage (see section 7)

7. Procedure for Planned Work Gone Awry or Expanding Outage
   a. Should any outage extend beyond the planned window or expand beyond the initial scope, the outage must be escalated to a higher severity level
      i. Procedures for unplanned outage (see section 5) take effect
         1. Primary contact may decide to open an entirely new outage or escalate existing outage depending on the scope of existing outage.
         2. Outage status can upgraded via web form, adhering to procedures outlined in section 3

8. Organizational Elements
   a. Planned event management
      i. Weekly planned event meeting (Monday 10AM) will be attended by directors of support and technical groups (or their designates) involved with current or ongoing work
         1. Planned work must be submitted via web (see section 6)
         2. All planned work must be approved by all at the meeting
      ii. Urgent planned events must be submitted via web (marked urgent)
         1. Approval from group director and PCSS director (or their designates), if at all possible
   b. Unplanned event management
      i. Outage is created by someone from the responsible servicing department (whoever is going to be working on the issue)
         1. Must adhere to update schedule according to severity (see section 5)
      ii. Outage is tracked by support center, who is responsible for pointing out any ambiguities or other concerns with regard to supporting clients
   c. Monitoring of IT infrastructure
      i. All relevant infrastructure elements are monitored by the Intermapper monitoring server
         1. All involved service departments (support, ITS-network, ITS-admin) must be able to query Intermapper for up/down status
         2. The Intermapper server is maintained by Network Services
         3. Infrastructure elements are mapped and grouped under three general categories, which can be used when assigning outage severity (per matrix in section 3)
            a. Medium-Low: (non essential but monitored)
            b. High: (non essential or essential-redundant)
            c. Critical services: essential to network operation and/or College business
               i. Modifications to the critical group are made by consensus at weekly CM meeting
               ii. Anyone involved in adding, moving or changing a critical service must also update monitoring for that service
               iii. Redundant services (from ‘High’ category) become critical if redundancy is lost (all services down)
   d. Monitoring responsibilities
      i. Viewers / Monitors
         1. Intermapper maps are accessible from the Web or from a licensed software application, authentication is required
         2. Any ITS personnel may request access to Intermapper
      ii. IT Support center
         1. Must have access to central monitoring systems and are able to verify, query or inquire about outages
      iii. Administrators (Server and Network admins)
1. Responsible for the devices and services that they manage
   a. keep them updated on the monitor server (if service is moved or changed in any way, they must update the associated monitoring element)
   b. ensure monitored elements send proper notifications (email, cell) where applicable
   c. communicate any monitoring changes to change management group