Major incident management process

Support team responsibilities
Objective

- Restore service with minimal downtime
- Regular updates to ensure effective communication
- Ensure and create an environment for support team to fully focus on the incident

Responsibilities

<table>
<thead>
<tr>
<th>Task</th>
<th>Is New?</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Service desk reports major incident to Major Incident Manager (MIM) on <strong>+61 3 992 52777</strong> and IT Support team via a positive handover (phone conversation with the MIM – do not leave a message on voicemail, <em>common sense, speak to line manager if you cannot get hold of MIM</em>) and VSM record and MIM assigns actions as appropriate</td>
<td>New</td>
</tr>
<tr>
<td>…or…. IT Support team on finding a suspected/potential major incident will log a Priority 1 (P1) or a Priority 2 (P2) incident record and conduct a positive handover to the MIM</td>
<td>New</td>
</tr>
<tr>
<td>Conduct thorough assessment</td>
<td>Current</td>
</tr>
<tr>
<td>Develop a service restoration plan and obtain approval from MIM</td>
<td>Current</td>
</tr>
<tr>
<td>Update progress to IT Helpdesk / MIM at regular intervals as agreed at the Plan of Action meeting</td>
<td>New</td>
</tr>
<tr>
<td>Carry out service restoration activities</td>
<td>Current</td>
</tr>
<tr>
<td>Prepare and document root cause of the incident</td>
<td>New</td>
</tr>
<tr>
<td>Monitor the impacted service</td>
<td>Current</td>
</tr>
</tbody>
</table>
Hours of coverage

• Major Incident Manager operates from 8am to 8pm
• The ICT Service Management Team will provide 12 hour coverage for any major incidents that occur during these hours
• Use +61 3 992 52777 to contact the Major Incident Manager (note: call may divert to IT Service Desk depending on time of day)

• Out of hours, **current “as is” process for each support team remains:**
  – Technical “on call” person notified by alerts
  – “On call” person fixes
  – Escalate to line manager if necessary

Note: Out of hours “as is” process varies between teams (to be standardised at a later date)
**Major Incident Management - Team Roles & Responsibilities**

### Incident
- **User Call**
  - Report Incident
  - Log incident record

- **IT Service Desk**
  - Log incident record

- **Major Incident Manager (MIM)**
  - **Yes** - Positive Handover of incident to MIM & On Call person
    - MIM to establish and validate Major Incident
    - Within 15 minutes
    - Send communications and assemble SRT
  - **No**
    - Continue with the Incident Management Process
    - Use priority matrix

- **Support Team**
  - **<<Trigger>>**
  - **Monitoring Tool, etc.**

#### Incident Categorisation
- **Is it a Major?**
  - **<<use priority matrix>>**
  - **NO**
    - Conduct Initial assessment to determine impacted services and users groups
  - **YES**
    - Preliminary Assessment and positive handover within 15 minutes of incident identification

#### Service Restoration Team (SRT) & Response Plan
- **Is Major?**
  - **NO**
    - Update Progress to MIM
    - Repeat at a frequency of 30 minutes or as agreed with MIM at the Plan of Action Meeting
  - **YES**
    - MIM to hold Plan of action meeting
    - SRT to conduct thorough assessment and develop response
    - Provide MIM with service restoration plan

#### Plan Execution
- **Approve service restoration activities**
- **SRT to execute the response**
- **Progress update to MIM at a regular interval as agreed**

#### MI Closure
- **Update Incident Record**
  - Prepare report within 5 days from Major incident resolved date
  - Circulate report to ILT
  - Problem management (notify, if applicable)
  - Initiate follow up with appropriate teams (if applicable)
  - Closure
  - Monitor the impacted services
  - Prepare root cause and Incident closure report
Evaluation

**Urgency x Impact = Priority**

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>University wide</td>
</tr>
<tr>
<td>Medium</td>
<td>Campus wide</td>
</tr>
<tr>
<td>Low</td>
<td>Building (50+)/Faculty</td>
</tr>
<tr>
<td></td>
<td>Floor/Lab (10+)/Course</td>
</tr>
<tr>
<td></td>
<td>Individual</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
<th>Priority Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Individual: P4, P4, P3</td>
</tr>
<tr>
<td>Medium</td>
<td>Floor/Lab/Course: P4, P3, P2</td>
</tr>
<tr>
<td>High</td>
<td>Building/Faculty: P3, P2, P1</td>
</tr>
<tr>
<td></td>
<td>Campus Wide: P3, P2, P1</td>
</tr>
<tr>
<td></td>
<td>University Wide: P3, P1</td>
</tr>
</tbody>
</table>

**Top 10**
- Peoplesoft
- SAP
- myRMIT / Learning Hub
- Blackboard
- Google Mail
- Staff Groupwise Mail
- VOIP
- Teaching Spaces (AV)
- Teaching Spaces (IT)
- EOL / STS

**Core**
- Network
- Load Balancers
- Storage
- NDS/AD
- DNS
- DHCP
- Firewalls
- etc...