IT Services

incident criteria

Guidance for IT Services staff on priorities to be used when logging incidents.

Table of Contents

Introduction .................................................................................................................. 2
Definitions ................................................................................................................... 2
Response time ............................................................................................................. 2
Resolution times .......................................................................................................... 2
Minimum information required from users .................................................................. 2
Changing the priority of incident tickets .................................................................... 3
Escalation .................................................................................................................... 3
Summary of response and resolution targets ............................................................... 4
Incident Criteria Matrix ............................................................................................. 5
Critical priority – reserved for major incidents ............................................................. 6
Urgent Priority ............................................................................................................ 6
High priority ............................................................................................................... 8
Low Priority .............................................................................................................. 9
**Introduction**

This document is to provide guidelines for setting the initial priority of incidents reported to IT Services and the expected response and resolution times.

This document will be updated as we get more data relating to incidents and as the Service Desk Improvement project progresses. If you have any comments on this document please contact Gordon Roberts or Steve Gough.

**Definitions**

<table>
<thead>
<tr>
<th>Incident</th>
<th>An unplanned interruption to an IT service or reduction in the quality of an IT service. Incidents may prevent users from working or reduce their effectiveness.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Request</td>
<td>A request from a user for information, or advice, or for a standard change or access to an IT Service. For example, to reset a password, or to provide standard IT Services for a new User.</td>
</tr>
</tbody>
</table>

**Response time**

The response time commences from when a call is logged by IT Services and a call reference number is allocated to the incident.

The response times apply to the standard University working hours only: Monday to Friday, 08:30-18:00.

For example, if a Low priority (response expected within 2 working days) call is received on Tuesday at 16:00, the target response time would be Thursday at 16:00.

**Resolution times**

Resolution time commences from when a call is logged by IT Services and a call reference number is allocated to the incident.

The response times apply to the standard University working hours only: Monday to Friday, 08:30-18:00.

IT Services will aim to resolve all incidents on a permanent basis, however sometimes it is necessary to find an interim solution (work around) in order to restore a service with a longer term solution following. For example if there was a faulty printer, an initial solution might be to use another printer, the permanent solution would be to repair or replace the faulty device. Resolution target times are therefore based on initial solution.

Where the solution is not permanent, IT Services staff will update the call as resolved or on hold but not closed until the permanent fix is in place. For example, if a printer stopped working and the workaround involved using an alternative printer, the call would be marked as ‘On Hold – See workflow diary’. The call would not be closed until the printer was repaired by an engineer and working fully again.

**Minimum information required from users**

When logging a call, all ITS staff recording an incident are expected to record the following minimum level of information:
- Name/user ID
- Telephone number
- Location
- University email address, or alternative email contact address
- Description of the incident (with as much detail as possible to aid with fixing the incident)
- An estimate of the impact caused by the incident and the number of users affected
- Relevant hardware or software details (e.g. IP address, MAC address) if applicable
- Depending on the type of incident, additional service related information may be required

In the new tool that will replace Remedy we may be able to “stop the clock” used to calculate response and resolution times until we have this data.

**Changing the priority of incident tickets**

Any member of staff may alter priority assignment on tickets if information obtained after incident was logged indicate that the initial priority was wrong.

If a ticket is deemed to be part of a major incident then this should be escalated, a major incident called and the (forthcoming) ITS major incident plan should be used to plan our response.

**Escalation**

With Remedy, ticket holders are notified of overdue tickets by email every Monday morning. With the Remedy replacement, we will be able to have the system automatically warn ticket holders of a potential breach of the target resolution time at 75% of the target time.
## Summary of response and resolution targets

<table>
<thead>
<tr>
<th>Priority</th>
<th>Target Response</th>
<th>Target Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>100% within 30 minutes</td>
<td>100% within 1 working day</td>
</tr>
<tr>
<td>Reserved for Major Incidents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Urgent</td>
<td>100% within 1 working hour</td>
<td>80% within 1 working day</td>
</tr>
<tr>
<td>High</td>
<td>100% within 1 working day</td>
<td>80% within 3 working days</td>
</tr>
<tr>
<td>Medium*</td>
<td>100% within 1 working day</td>
<td>80% in 5 working days</td>
</tr>
<tr>
<td>Low</td>
<td>100% within 2 working days</td>
<td>80% within 5 working days</td>
</tr>
<tr>
<td>Requests for services</td>
<td>As specified in SLA for service</td>
<td>As specified in SLA for service</td>
</tr>
</tbody>
</table>

*Medium category is solely reserved for Reading Connect tickets and may not be used for any other category of ticket. This priority is not described below.*
Incident Criteria Matrix

For each incident, verify the extent and impact and select the appropriate code. Use these two codes to work out the appropriate priority.

Extent
1. Whole campus, major service, event or process
2. Large group of users, a group of VIPs, a service or event
3. Small group of users or a VIP
4. Single user

Impact
A. Critical work impossible or life, security or reputation at risk
B. Some work impossible or moderate health, security or reputation implications
C. Reduced efficiency or minor health, security or reputation implications
D. Inconvenience

Examples
The entire email service (1) is not useable (A) = Critical
An entire team (3) can’t access a shared drive (B) = Urgent
The Wren service (2) is running slowly (C) = High
A single user (4) has to type their password every time they open Outlook (D) = Low
Someone (4) who relies on their phone to do their job can’t make calls (A) = Urgent
A cable creating a possible trip hazard (C) is identified in a single occupancy office (4) = Low
All computer users (1) have to type their password to access the internet (D) = High
Critical priority – reserved for major incidents

**Description**
An incident that satisfies any of the following criteria:

- Prevents the effective use of any major service, i.e. email, Internet, Blackboard, RISIS, finance software etc by a large number of users (e.g. all users, whole campus)
  - especially if it occurs during a critical time (e.g. during an examination period, new student intake, clearing, end of financial year)
- Implies a serious breach of security – e.g. compromise of large amount of (personal) data.
- Has a serious implication for the reputation of the University
- Has an immediate and potentially serious health and safety implication

**Response target**
To respond to 100% of incidents within 30 minutes.

**Resolution target**
To resolve 100% of incidents within 1 day.

**Updates**
The ITS Major Incident Manager will keep key IT Services staff updated (e.g. ITS Directorate and senior managers) and will co-ordinate regular updates to stakeholders (e.g. departmental managers and Heads of School).

For major incidents affecting a significant number of users, the latest information will be provided on the ITS Status Page.

**Escalation**
All Critical incidents will immediately be escalated to a senior ITS manager and a Major Incident Manager will be designated to deal with the major incident. The Major Incident Manager will follow the ITS Major Incident Plan.

All major incidents will be reviewed promptly after their resolution.

**Examples**
- Major University System failure e.g. email, Blackboard, RISIS, file servers, external web site
- Complete or significant loss of campus network connectivity
- Complete or significant loss of the telephone network
- A network problem on the readingConnect service which affects an entire hall or several halls
- A significant, malicious, security attack
- Fire/flood of a building

**Urgent Priority**

**Description**
An incident that satisfies any of the following criteria:
• Prevents the effective use of any service and affects a substantial number of computer users, telephones or lecture/conference rooms
• Impacts an important business critical process
• Implies a breach of security
• Has possible implications for the reputation of the University
• Has very serious implications for an individual user
• Has moderate health and safety implications

Response target
To respond to 100% of incidents within 1 working hour.

Resolution target
To resolve 80% of incidents within 1 working day.

Updates
If appropriate (e.g. if the incident affects a significant number of users), the latest information will be updated on the ITS Status Page.

Examples
• Server down that prevents a group of users from being able to operate as normal (i.e. inhibits their usual business processes)
• Degradation of Internet connectivity affecting a group of users (e.g. 50 people or more)
• Department file share out of file space
• Printer not working that affects many users without alternative printer available
• Partial loss of campus network access or telephone connectivity unavailable in a building
• A crucial PC that is down and is used for teaching (e.g. lecture theatre PC affecting a substantial number of attendees)
• A network problem on the readingConnect service which affects 20 or more rooms
• VIPs affected
High priority

Description
An incident that satisfies any of the following criteria:

- Causes inconvenience to a small number of computer users, telephone or a lecture theatre presentation
- An important service is available but performance is poor
- Affects the provision of teaching and learning for a class or meeting
- Has minor health and safety implications

Response target
To respond to 100% of incidents within 1 working day.

Resolution target
To resolve 80% of incidents within 3 working days.

Updates
For incidents affecting a significant number of users, updates will be placed on the ITS Status Page.

Examples
- Telephone or Network fault affecting an office with multiple occupancy
- A team unable to send or receive vital work-related email via a group account
- Group printer unavailable
- Email slow for a small number of users
Low Priority

Description
An incident that satisfies any of the following criteria:

- Causes inconvenience to an individual
- A "limited support" category, for example an external SLA for non-essential equipment
- Small impact on business operations for an individual

Response target
To respond to 100% of incidents within 2 working days.

Resolution target
To resolve 80% of incidents within 5 working days.

Updates
Users will be able to contact the IT Service desk for any updates to the incident.

Examples
- A user requires assistance with modifying a Word document in a particular way
- A user having problems with a setting that is inconvenient but does not stop them working
- Single user PC not working correctly (e.g. an application problem)
- A problem on readingConnect affecting a single user